SCHRIFTEN DES IRDT

TRIER STUDIES ON DIGITAL LAW

Benjamin Raue (Hrsg.)

Digitale Resilienz: Effektives Recht auf sichere Software

Volume 3

Benjamin Raue (Hrsg.)

Digitale Resilienz

Effektives Recht auf sichere Software

SCHRIFTEN DES IRDT

Herausgegeben vom Verein für Recht und Digitalisierung e.V.
Institut für Recht und Digitalisierung Trier (IRDT)

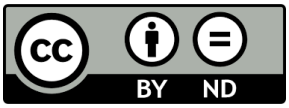
Trier, 2024
Volume 3

SCHRIFTEN DES IRDT

TRIER STUDIES ON DIGITAL LAW

Herausgegeben vom Verein für Recht und Digitalisierung e.V.,
Institut für Recht und Digitalisierung Trier (IRDT), Behringstr. 21, 54296 Trier, Deutschland

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.
Dieses Buch ist ebenfalls als E-Book verfügbar unter: https://www.epubli.com/shop



ISBN: 9783758493089
URN: urn:nbn:de:hbz:385-2024031307
DOI: https://doi.org/10.25353/ubtr-42d2-df9e-f813

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).

UNIVERSITÄT TRIER

IRDT Institute for Digital Law Trier

Inhaltsverzeichnis

Einleitung

Digitale Resilienz: Effektives Recht auf sichere Software?

Benjamin Raue

A. Analoge und digitale Sicherheit

In analogen Systemen ist Sicherheit sichtbar und fühlbar: Schlösser, Mauer oder Wachpersonal. Diese sichtbare Sicherheit ist aber oft nur eine gefühlte Sicherheit. Denn jedes System ist letztlich überwindbar. Das wissen wir seit Menschengedenken und das heute noch präsente Beispiel stammt aus der griechischen Mythologie. Das Trojanische Pferd (und mit ihm griechische Soldaten) konnte mit List und Tücke Mauern überwinden, die mit damaligen militärischen Mitteln nicht zu überwinden waren. Digitale Systeme sind nicht per se leichter zu durchdringen, auch wenn es das geflügelte Wort gibt, dass eine Software nicht fehlerfrei programmiert werden kann.[1] Aber wenn sie an das Internet angeschlossen sind, können sie zum einen von jedem Ort der Welt und – wenn dasselbe (Sicherheits-)Systeme an vielen verschiedenen Stellen eingesetzt wird – skalierbar überwunden werden. Wenn ein Angreifer einmal eine Sicherheitslücke entdeckt hat, dann weiß er nicht nur, wie er die Mauern von Troja überwinden kann, sondern auch, die Mauern von Universitäten, Krankenhäusern und Unternehmen. Zudem muss er nicht mehr nach Troja – oder Trier, Erfurt bzw. München – reisen oder ein Holzpferd als Ablenkung mitnehmen, um in sichere Umgebungen einzudringen. Die Angreifer sind also örtlich viel unabhängiger.

Diese neue Verwundbarkeit führt zu neuen Geschäftsmodellen von Cyberkriminellen und vielen öffentlichkeitswirksamen Cyberangriffen. So z.B. im Fall einer bekannten Hotelkette, bei der viele der Tagungsteilnehmer schon zu Gast waren, und die Opfer eines Hackerangriffs wurde. Da sie nicht bereit war, das geforderte Lösegeld zu zahlen, sind nun deren Businesspläne und viele Übernachtungs- und andere persönliche Daten ihrer Hotelgäste im Darknet zu finden. Auch die Universität Gießen war einen Monat lang komplett offline und alle IT-Systeme mussten neu aufgesetzt werden. Die Beispiele sind Ausdruck dafür, dass Cyberangriffe überall und jederzeit passieren – und fast jeden treffen können.

[1] S. dazu schon *BSI*, Sicherheitsbericht 2015, S. 10; *Raue*, NJW 2017, 1841.

B. Recht auf sichere Software

Cyberattacken sind untrennbar verbunden mit der Frage nach einem effektiven Recht auf sichere Software. Der BSI-Sicherheitsbericht 2023 sieht die größte Sicherheitsbedrohung für Wirtschaft und öffentliche Verwaltung in Ransomware-Angriffen, die – nicht nur, aber auch – dadurch ermöglicht werden, dass Sicherheitslücken in Software existieren und nicht zeitnah geschlossen werden.[2] Das Thema effektives Recht auf sichere Software ist daher dauerhaft aktuell und von immer größerer Bedeutung.

Aus dem Sicherheitsbericht des BSI geht auch hervor, dass im Jahr 2023 rund ein Viertel mehr Sicherheitslücken gefunden wurden als im Jahr 2022.[3] Entweder die Bedrohungslage oder zumindest die Aufmerksamkeit für dieses Thema nimmt also zu. Beunruhigend ist auch, dass im Sicherheitsbericht von 2023 15 Prozent der gefundenen Schwachstellen als kritisch eingestuft wurden.[4]

Es ist daher sowohl von individueller als auch von gesellschaftlicher Bedeutung, dass Sicherheitslücken geschlossen werden.[5] Das ist jedoch nicht immer der Fall. Nicht selten werden sogar neue Produkte mit bekannten Sicherheitslücken auf den Markt gebracht.[6]

Deshalb haben wir auf der Jahrestagung des IRDT am 12. und 13.10.2023 diskutiert, wie das Recht effektiv sicherstellen kann, dass Sicherheitslücken geschlossen werden. Natürlich besteht jedenfalls für den Hersteller eine entsprechende Verkehrspflicht, keine unsichere Software auf den Markt zu bringen[7] – und nachträglich auftretende Sicherheitslücken zu schließen. Das legen *Thomas Riehm, Malte Leithäuser* und *Raphael Brenner* in ihrem Beitrag „Recht auf sichere Software: Vertragliche Ansprüche auf Sicherheitsaktualisierungen?“ dar und zeigen hier insbesondere auf, wie sich die neuen vertraglichen Regeln über digitale Produkte auswirken (S. 5-38). Hierbei nehmen die Autoren in ihrem Beitrag die in Betracht kommenden vertraglichen Ansprüche in den Fokus und gehen auf die Frage ein, wann eine Software mangelfrei ist. Sie führen aus, wie ein Verkäufer, der nicht gleichzeitig Hersteller ist, einen Nacherfüllungsanspruch in der Realität umsetzen könne. Eine Software könne faktisch zwar nie frei von Mängeln sein. Trotzdem werde ein angemessenes Sicherheitsniveau geschuldet,

---

[2] BSI, Die Lage der IT-Sicherheit in Deutschland 2023, S. 11, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf.

[3] BSI, Die Lage der IT-Sicherheit in Deutschland 2023, S. 46, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf.

[4] BSI, Die Lage der IT-Sicherheit in Deutschland 2023, S. 46, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf.

[5] Dazu auch schon *Raue*, NJW 2017, 1841.

[6] S. etwa OLG Köln MMR 2020, 248.

[7] Vgl. BGH NJW 1990, 906 (908). Anders dagegen für Elektronikmarkt, nicht ganz unumstritten, OLG Köln MMR 2020, 248 m. abl. Anm. Riehm/Meier.

für dessen Erreichen sich der Verkäufer ggf. Dritter, etwa dem Hersteller, bedienen müsse.

Christian Ernst behandelt in seinem Beitrag übergreifend, welche Verantwortung der Staat für sichere Software hat (S. 39-56). Es sei für den Staat grundrechtlich geboten, den Schutz der öffentlichen Sicherheit zu stärken, jedoch existiere kein pauschales Recht auf sichere Software. Der Schutz des Individuums müsse im Einzelfall anhand der einschlägigen Grundrechte geprüft werden. Die Verantwortung für IT-Sicherheit liege nicht allein bei staatlichen Stellen, vielmehr wirkten sie ergänzend.

Einen ganz anderen Aspekt von sicherer Software behandelt *Thomas Wischmeyer*. Er untersucht, ob der Staat erkannte IT-Sicherheitslücken verschweigen und für eigene Zwecke nutzen darf – und entwirft dabei die rechtlichen Grundzüge des staatlichen Schwachstellenmanagements (S. 57-78). Staatliche Stellen sollten nicht nur das Handeln Privater in den Blick nehmen, sondern auch ihr eigenes Verhalten zu IT-Sicherheitslücken auf einen kritischen Prüfstand stellen. Insbesondere seien insofern verbindliche Regeln im Umgang mit solchen Schwachstellen erforderlich.

C. Effektive Rechtsdurchsetzung

Es bleibt dann aber in der Praxis die wesentliche Frage, wie diese Pflichten durchgesetzt werden können. Auch dieser Frage nähern wir uns aus einer intradisziplinären, privatrechtlichen und öffentlich-rechtlichen Perspektive. Das ist deshalb fruchtbringen, weil – stark vereinfacht – öffentliche Akteure besonders geeignet sind, etablierte Verhaltensregeln gleichmäßig und flächendeckend durchzusetzen, während private Akteure zwar nur punktueller, dafür aber oft risikofreudiger sind und flexibler agieren.

Anschaulich gemacht hat dies der Bereich des Datenschutzes, wo der Max-Schrems-Effekt beobachtet werden kann: Er hat die DSGVO an politisch sensiblen Stellen – insbesondere beim Datenaustausch mit den USA – durch private Klagen auf den Prüfstand gestellt. Am Ende hat der EuGH entschieden, dass die Abkommen mit den USA nicht das Niveau haben, das wir in der EU vereinbart haben. Diesen Schluss konnten oder wollten die Datenschutzbehörden nicht ziehen. Gleichzeitig können einzelne Akteure nicht in der Breite und so konsistent die Vorgaben des Datenschutzes durchsetzen, wie Behörden es tun können. Das zeigt, dass beide Formen der Rechtsdurchsetzung ihre Stärken haben.

Steve Ritter vom Bundesamt für Sicherheit in der Informationstechnik schildert in seinem Beitrag, welche Befugnisse dem Amt ermöglichen, Sicherheitsanforderungen einheitlich und flächendeckend durchzusetzen (S. 79-96). So betonte er die Bedeutung eines geschützten Rahmens zur Meldung von bislang unbekannten Sicherheitslücken. Es müsse sichergestellt werden, dass keine negativen Folgen für den Meldenden zu befürchten seien, die ihn von einer Meldung abhalten könnten. Zudem ging er darauf ein,

dass es nicht unbedingt zielführend sei, jede Schwachstelle sofort publik zu machen, etwa wenn technisch noch keine Lösung zur Verfügung stehe. Er appellierte an den Einzelnen, alle einfachen Maßnahmen, wie etwa regelmäßige Updates oder sichere Passwörter, konsequent umzusetzen, um so die Sicherheitslage erheblich zu verbessern.

Anschließend wirft *Wiebke Voß* einen zivilprozessualen Blick auf die effektive Durchsetzung vertraglicher Ansprüche in der Praxis. In der Vergangenheit bestand fast Einigkeit darin, dass es zwar Ansprüche auf Schließung von Sicherheitslücken gab, diese aber faktisch nicht durchsetzbar waren. Voß zeigt auf, dass es nun mit dem Gesetz zur gebündelten Durchsetzung von Verbraucherrechten (VDuG) insbesondere kollektive Möglichkeiten zur Durchsetzung privater Ansprüche auf Sicherheitsupdates gibt (S. 97-114). Sie hebt dabei die Abhilfeklage hervor, eine Art kollektiver Leistungsklage zur gerichtlichen Geltendmachung der verfolgten Interessen. Problematisch sei, dass der zu befürchtende Aufwand und ein Mangel an konkret verwertbaren Informationen viele Nutzer vermutlich von einer Durchsetzung auf dem Klageweg abhalten wird.

In seinem abschließenden Beitrag skizziert *Christian Armbrüster* wie privatrechtliche Vereinbarungen in Form von Versicherungsverträgen rechtliche und faktische Anreize setzen und der Wissensvorsprung von Versicherungen wie Versicherungsmaklern genutzt werden kann, um das Sicherheitsniveau von privat genutzten IT-Systemen zu erhöhen (S. 115-129). Versicherungen geben ihren Vertragspartnern in den Versicherungsbedingungen ein bestimmtes Verhalten bei der IT-Sicherheit verbindlich vor. Die damit verbundene Anreizwirkung verbessere die Sicherheitslage insgesamt erheblich. Zudem steige auf Seiten der Versicherten das Bewusstsein für die Gefahrenlage und die Notwendigkeit angemessener Maßnahmen.

Kapitel 1: Recht auf sichere Software?

Vertragliche Ansprüche auf Sicherheitsaktualisierungen?

Thomas Riehm, Malte Leithäuser und Raphael Brenner

Seit dem 01.01.2022 gelten die Regelungen über die sog. „Aktualisierungspflicht“ im vertraglichen Verhältnis zwischen Verbrauchern und Unternehmern bei Verträgen über digitale Produkte (§ 327f BGB) und bei Kaufverträgen über Waren mit digitalen Elementen (§ 475b IV Nr. 2 BGB). Zugleich wurde erstmals die „Sicherheit“ des digitalen Produkts wie auch der Kaufsache ausdrücklich als Element der geschuldeten objektiven Sollbeschaffenheit gesetzlich erfasst (§§ 327e III 1 Nr. 2, 434 III 2 BGB). Der nachfolgende Beitrag geht der Frage nach, inwieweit diese Vorschriften – und andere privatrechtliche Regelungsinstrumente – in der Lage sind, die „digitale Resilienz“ von Geräten im Internet of Things (IoT-Geräte) und sonstigen Softwareprodukten zu erhöhen, indem sie praktisch wirksame Ansprüche auf Sicherheitsaktualisierungen gewähren, die vorhandene Sicherheitslücken schließen können.

Dabei besteht ein vielfältiges System von Rechtsgrundlagen, aus denen sich privatrechtliche Ansprüche von Software-Nutzern sowie Nutzern von IoT-Geräten auf die Bereitstellung von Sicherheitsaktualisierungen ergeben können. Zu unterscheiden sind insoweit auf der einen Seite gesetzliche Ansprüche gegen Softwarehersteller und auf der anderen Seite vertragliche Ansprüche gegen den jeweiligen Vertragspartner, der mit dem Softwarehersteller häufig nicht identisch ist. Die gesetzlichen Vorgaben für das Verbrauchervertragsrecht unterscheiden sich zudem erheblich zu denen für den B2B-Verkehr. Das gilt auch für Ansprüche auf Sicherheitsaktualisierungen.

A. Gesetzliche Ansprüche gegen Softwarehersteller

Gesetzliche Ansprüche der Nutzer von IoT-Geräten oder Softwareprodukten gegen deren Hersteller können sich aus dem allgemeinen Produkthaftungsrecht ergeben, das in § 823 I BGB sowie im Produkthaftungsgesetz geregelt ist.

I. Informationssicherheit als Element des produkthaftungsrechtlichen Fehlerbegriffs

In welcher Weise Anforderungen an die Informationssicherheit vom produkthaftungsrechtlichen Fehlerbegriff umfasst sind und der Hersteller daher die „digitale Resilienz" seiner Softwareprodukte gewährleisten muss, ist jedoch unklar und umstritten. Insbesondere gilt das für die Frage, inwieweit Softwarehersteller auch für Cyberangriffe Dritter, die auf Sicherheitslücken der im Produkt verwendeten Software zurückzuführen sind, verantwortlich im Sinne des Produkthaftungsrechts sind.

Dies führt im Ausgangspunkt zu der Unterscheidung zwischen *safety* und *security*: Traditionell beziehen sich Anforderungen an die Produktsicherheit auf den Schutz des Nutzers oder Dritter vor von dem Produkt ausgehenden Gefahren (*safety*). Dem steht die Informationssicherheit gegenüber, also die Sicherheit des Softwareprodukts selbst gegenüber inneren und äußeren Einflüssen (*security*).[1] *Security* betrifft die Einhaltung von Sicherheitsstandards zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit von Informationen (vgl. § 2 II 4 BSIG). Dadurch soll der Schutz des Produkts vor Eingriffen oder Manipulationen Dritter sichergestellt werden (*Resilienz*).[2] Eine erhebliche Gefahr für die Informationssicherheit bilden Software-Sicherheitslücken. Dabei handelt es sich um Softwareeigenschaften, durch die sich Dritte unberechtigten Zugang zu informationstechnischen Systemen verschaffen oder deren Funktion beeinflussen können (§ 2 VI BSIG).[3] Spätestens mit der Implementierung von Software in physische Produkte beschränken sich Gefährdungen durch das Ausnutzen von Sicherheitslücken nicht mehr auf die Schutzgüter der *security*. Vielmehr kann ein Zugriff Integritätsschäden und damit wiederum *safety*-relevante Gefahren nach sich ziehen.[4] Damit kann aber auch bei der Frage des haftungsrechtlichen Schutzumfangs an dieser Stelle nicht stehengeblieben werden. Denn wo eine Gefahr für die Schutzgüter der *security* in eine Gefahr für die Schutzgüter der *safety* umschlagen kann, wo *security* und *safety* also verschmelzen, entstehen Gefährdungen, die klassischerweise dem Rechtsgüterschutz des Produkthaftungsrechts unterfallen.[5] Da diese Gefährdungen

[1] Zu den Begriffen von *safety* und *security*: *Kipker*, in: Kipker (Hrsg.), Cybersecurity, 2. Aufl. 2023, Kap.1 Rn. 6; *Fedler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, 91 (99); plakativ und bewusst zur vereinfachten Gegenüberstellung von *safety* als „Schutz der Umwelt vor Systemen" und *security* als „Schutz der Systeme vor der Umwelt": *Grimm/Waidner*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2020, § 2 Rn. 4.

[2] Dazu *Bräutigam/Klindt*, NJW 2015, 1137 (1141).

[3] Dazu auch *Ritter*, Kapitel 2 in diesem Band.

[4] *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, 2023, 89 sprechen davon, dass die IT-Sicherheit mittelbar der Produktsicherheit dient und sich als Teilaspekt des Produktsicherheitsrechts entpuppt.

[5] *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, 2019, 193; *Wiebe*, InTer 2020, 66 (67); NK-ProdR/*Ackermann*, 2022, § 823 BGB Rn. 22; *Raue*, NJW 2017, 1841 (1843).

auch von einer ausnutzbaren Sicherheitslücke ausgehen können, lassen sich *security* und *safety* im Bereich von Software gar nicht mehr voneinander trennen. Sie verschmelzen zu einem einheitlichen Begriff von Informationssicherheit als Anforderung des Produktsicherheits- und des Produkthaftungsrechts.[6]

Dass es sich bei einem Hackerangriff um eine bewusste und vorsätzliche Schädigung eines Dritten handelt, schließt die Verantwortlichkeit des Herstellers dabei nicht aus.[7] Auch im allgemeinen Deliktsrecht ist anerkannt, dass das vorsätzliche Dazwischentreten Dritter die Zurechnung nicht stets ausschließt. Vielmehr bleibt eine Zurechnung möglich, wenn eine besondere Gefahrenlage geschaffen wurde, die über das allgemeine Lebensrisiko hinausgeht und die Dritteinwirkung ermöglicht oder zumindest wesentlich erleichtert hat.[8] Übertragen auf Cyberangriffe besteht bei einer bei Inverkehrgabe vorhandenen Sicherheitslücke, die ein mögliches Einfallstor für Hacker darstellt, eine latente und vom Hersteller zu verantwortende besondere Gefahrenlage, die eine schädigende Handlung Dritter erst ermöglicht oder zumindest wesentlich erleichtert. Im Rahmen des Produkthaftungsrechts trifft die Hersteller damit eine Verkehrspflicht, auch die *security* ihrer Produkte sicherzustellen. Kommen sie dieser Verpflichtung nicht nach, haften sie auch für Schäden, die dadurch entstehen, dass Dritte die durch die Sicherheitslücke vorhandene latente Produktgefahr vorsätzlich ausnutzen.[9]

II. Produkthaftungsrechtliche Aktualisierungspflicht

Das Produkthaftungsrecht normiert Aktualisierungspflichten (bislang[10]) nicht ausdrücklich. Es regelt im Ausgangspunkt nur Schadensersatzansprüche der Nutzer sowie

---

[6] Im Englischen „safety-relevant cybersecurity", dazu *Kapoor/Klindt*, BB 2023, 67 (68); *Wiebe*, BB 2022, 899 (900); *Wiesner*, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 10.6 Rn. 244; *Freiling/Grimm/Großpietsch u.a.*, Informatik Spektrum 37 (2014), 14, (19, 22); *Schneider/Trapp/Dörr u.a.*, Informatik Spektrum 40 2017, 419 ff.: „umfassendes Sicherheitsverständnis"; kritisch aber *Hartmann/Klindt*, ZfPC 2022, 73 (73 f.).

[7] S. zu dieser Frage wie hier *Spindler*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, § 11 Rn. 24; *Raue*, NJW 2017, 1841 (1843); zurückhaltend *Klindt*, DAR 2023, 7 (9).

[8] Vgl. zu diesen allgemeinen Erwägungen der Kausalitätslehre MüKoBGB/*Oetker*, 9. Aufl. 2022, § 249 Rn. 157 ff.; BeckOK BGB/*Flume*, 68. Ed. 01.11.2023, § 249 Rn. 311; speziell im haftungsrechtlichen Kontext MüKoBGB/*Wagner*, 9. Aufl. 2024, § 823 Rn. 539 f.; BeckOGK BGB/*Spindler*, 01.12.2023, § 823 Rn. 425.

[9] *Wiebe*, InTer 2020, 66 (68); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, 90 f.; *Spindler*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, § 11 Rn. 24; zurückhaltend aber *Steege*, SVR 2023, 9 (14).

[10] Künftig wird die neue Produkthaftungsrichtlinie (vgl. Europäisches Parlament, Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 12.03.2024 im Hinblick auf den Erlass der Richtlinie (EU) 2024/... des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, https://europarl.europa.eu/doceo/document/TA-9-2024-0132_DE.pdf (geprüft am 15.03.2024)) jedenfalls implizit zu einer produkthaftungsrechtlichen Updatepflicht des Herstellers zur Aufrechterhaltung der Produktsicherheit

Dritter gegen den Hersteller für den Fall der Verletzung eines geschützten Rechtsguts aufgrund eines anfänglichen Produktfehlers. Die Rechtsprechung hat hieraus im Rahmen des § 823 I BGB indes auch eine präventive Pflicht der Hersteller zur Vermeidung von Rechtsgutsverletzungen aufgrund erst später, also nach Inverkehrgabe, erkannter Produktgefahren abgeleitet. Die sog. Produktbeobachtungspflicht verpflichtet den Hersteller dazu, auch nach Inverkehrbringen des Produkts zu beobachten, ob sich „im Feld" sicherheitsrelevante Produktgefahren zeigen, und ggf. hierauf zu reagieren.[11]

1. Verhältnis der Gefahrenabwehrmaßnahmen zueinander

Bei der Bestimmung der Herstellerpflichten zur Abwehr dieser Gefahren ist allerdings zu beachten, dass das Produkthaftungsrecht ausschließlich dem Rechtsgüterschutz beim Nutzer und bei Dritten dient (*Integritätsinteresse*). Nicht geschützt ist dagegen das Interesse der Nutzer an einem funktionsfähigen Produkt (*Äquivalenzinteresse*); dieses Interesse wird allein durch das Vertragsrecht geschützt, welches dem Nutzer Ansprüche gegen seinen Vertragspartner gewährt. Die produkthaftungsrechtlichen Pflichten des Herstellers sind daher grundsätzlich auf Maßnahmen zur Vermeidung von Rechtsgutsverletzungen beschränkt.[12] Solche Maßnahmen können etwa die Warnung der Nutzer, aber auch die Auslieferung von Softwareaktualisierungen oder bei physischen Geräten eine Reparatur sein. Denkbar ist daneben die völlige Abschaltung von Software bzw. bei Hardware der Rückruf, um das Produkt aus dem Verkehr zu ziehen.[13]

Die Frage, ob bzw. unter welchen Voraussetzungen der Hersteller von Softwareprodukten Aktualisierungen zur Gefahrenabwehr bereitstellen muss, betrifft den Kern der Abgrenzung des Integritäts- vom Äquivalenzinteresse. Zwar ist eine Warnung des Herstellers grundsätzlich ausreichend, um das deliktsrechtlich ausschließlich geschützte Integritätsinteresse des Nutzers zu wahren. Besteht aber Grund zur Annahme, dass sich

führen. Denn selbst wenn der Hersteller nachweisen kann, dass der schadenursächliche Fehler des Produkts zum Zeitpunkt des Inverkehrbringens wahrscheinlich noch nicht vorlag, soll er sich nicht entlasten können, wenn das Fehlen von zur Aufrechterhaltung der Sicherheit erforderlichen Software-Updates oder -Upgrades zur Fehlerhaftigkeit des Produkts geführt hat; vgl. dazu *Wagner*, JZ 2023, 1 (7); *Spindler*, CR 2022, 689 (694).

[11] Grundlegend BGH NJW 1981, 1606 (1607 f.) und BGH NJW 1981, 1603 (1604); vgl. auch NK-ProdR/*Ackermann*, § 823 BGB Rn. 116; BeckOK BGB/*Förster*, § 823 Rn. 735.

[12] Vgl. BGH NJW 2009, 1080 (1082) m.w.N.

[13] § 2 Nr. 24 ProdSG definiert Rückruf als „jede Maßnahme, die auf Erwirkung der Rückgabe eines dem Endnutzer bereits bereitgestellten Produkts abzielt" (s.a. BGH NJW 2009, 1080 (1081) zur Vorgängerregelung in § 2 XVII GPSG a.F.). Die Reparatur des fehlerhaften Produkts durch Hersteller oder Vertragshändler, die etwa im Automobilsektor üblich ist (vgl. dazu *Lüftenegger*, DAR 2016, 122 (122)), ist hiervon nicht umfasst, sondern wird regelmäßig freiwillig als Marketinginstrument eingesetzt, auch wenn keine gesetzliche Verpflichtung dazu besteht.

der Nutzer über die Warnung hinwegsetzt und dadurch Dritte gefährdet, kommen weitergehende Sicherungspflichten des Herstellers in Betracht.[14] Aufgrund der tatsächlichen Gegebenheiten bei Softwareprodukten ist hier ein Hinwegsetzen über eine Warnung gerade deswegen denkbar, weil es den Nutzern nicht zumutbar ist, die Gefahr selbst zu steuern.

2. Bereitstellung von Softwareaktualisierungen

Diese Unzumutbarkeit kann sich daraus ergeben, dass der Nutzer selbst nicht in der Lage ist, Sicherheitslücken zu beseitigen, während der Hersteller auch nach dem Zeitpunkt der Inverkehrgabe noch gesteigerte Einflussmöglichkeiten besitzt. Da allein der Hersteller den Aufbau und die Konzeption der Software in Gänze versteht, ist er regelmäßig der einzige Akteur, der Fehler beheben und die Software sicher(er) machen kann.[15] Bei der Gefahrenbeseitigung durch eine Behebung des ursprünglichen Fehlers ist der Nutzer damit auf den Hersteller und von ihm bereitgestellte Aktualisierungen angewiesen.[16] Wegen der fehlenden Möglichkeit des Nutzers, die Sicherheitsmängel selbst oder unter Zuhilfenahme Dritter als Fachleute zu beheben, ist die Warnung in diesen Fällen ein wenig wirksames Mittel der Gefahrenabwehr.[17] Denn in solchen Konstellationen verbleibt dem Nutzer keine andere Möglichkeit, als im Rahmen der Gefahrensteuerung auf die Nutzung des Produkts zu verzichten.[18] Bei Produkten, die für die Lebensführung von zentraler Bedeutung sind,[19] ist ein Nutzungsverzicht aber kaum zu erwarten. Angesichts der allgegenwärtigen Fehleranfälligkeit von Software gilt dies dort umso mehr.[20] Hinzu kommt, dass die Abhängigkeit des Nutzers bei der Fehlerbehebung vom Hersteller mit erhöhten Einflussmöglichkeiten des Herstellers auf das Produkt auch nach dem Inverkehrbringen korrespondiert.[21] Da Softwareprodukte über das Internet verbunden sind, können die Hersteller jederzeit aus der Ferne auf ihre Produkte zugreifen und auf die sicherheitsrelevanten Eigenschaften per Aktualisierung Einfluss nehmen, sodass diese weiterhin ihrer Kontrolle unterliegen.[22] Im

[14] BGH NJW 2009, 1080 (1081).

[15] *Regenfus*, JZ 2018, 79 (80); *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-HdB, 37. Aufl. 2022, 50.1 Rn. 460.

[16] *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, 2021, 241; *Sommer*, Haftung für autonome Systeme, 2020, 280.

[17] *Gomille*, JZ 2016, 76 (80).

[18] *Raue*, NJW 2017, 1841 (1842 f.).

[19] Vgl. zu diesem Kriterium *Rudkowski*, VersR 2018, 65 (72); *Lüftenegger*, NJW 2018, 2087 (2090).

[20] *Oster*, in: Foerste/Graf v. Westphalen (Hrsg.), Produkthaftungshandbuch, 4. Aufl. 2024, § 57 Rn. 26 sieht in einer Updatepflicht der Hersteller gerade die Kehrseite dieser Fehleranfälligkeit von Software.

[21] *Schrader*, in: Buck-Heeb/Oppermann (Hrsg.), Automatisierte Systeme, 2022, 333 (334).

[22] *Riehm*, in: Verhandlungen des 73. Deutschen Juristentages, Band II/1, 2023, K47 (K 56); *Thöne*, Autonome Systeme, 2020, 215; *Mayrhofer*, Außervertragliche Haftung für fremde Autonomie, 2023, 291 f.; *Sommer*, Haftung für autonome Systeme, 280.

Vergleich zur Nachrüstung körperlicher Gegenstände ist die Bereitstellung von Softwareaktualisierungen zudem mit geringem Aufwand und geringen Kosten für den Hersteller möglich.[23] Die vorzunehmende Einzelfallbetrachtung kann bei Softwareprodukten daher zu einer Pflicht des Herstellers führen, Aktualisierungen bereitzustellen. Hierin liegt auch keine systemwidrige Ausweitung des Äquivalenzinteresses im Bereich des Deliktsrechts; vielmehr handelt es sich um die Folge einer am Integritätsschutz ausgerichteten effektiven Gefahrenabwehr.[24]

3. Zwangsaktualisierung und Deaktivierung des Geräts als ultima ratio

Im Extremfall kann es auch der produkthaftungsrechtlichen Präventionspflicht eines Herstellers entsprechen, ein Gerät oder eine Software vollständig abzuschalten, um die hiervon ausgehenden Gefahren für geschützte Rechtsgüter zu vermeiden.[25] Dass die Nutzer dann kein funktionsfähiges Produkt mehr haben, ist aus produkthaftungsrechtlicher Perspektive unerheblich, weil es insoweit nur darauf ankommt, dass von dem Produkt keine Gefahren für geschützte Rechtsgüter mehr ausgehen. Im Hinblick auf die mangelnde Funktionsfähigkeit müssen sie sich allein mit ihrem Vertragspartner auseinandersetzen und beispielsweise gewährleistungsrechtliche Rechtsbehelfe geltend machen, sofern diese noch nicht verjährt sind. Freilich wird das nur eine Notlösung in absoluten Ausnahmefällen sein, weil eine solche Komplettabschaltung für die Reputation des Herstellers desaströs wäre.

Jeglicher nachträgliche Eingriff des Herstellers in das Produkt steht zudem potenziell im Konflikt mit dem Eigentumsrecht des Nutzers.[26] Auch die nachträgliche Veränderung von Software auf einem Gerät, das im Eigentum des Nutzers steht, verletzt dieses Eigentum;[27] erst recht gilt das für die Totalabschaltung des Geräts bzw. der Software. Rechtlich zulässig ist das daher nur mit Einwilligung des Nutzers oder aufgrund eines besonderen Rechtfertigungsgrunds.[28]

Diese Konfliktlage hat Rückwirkungen auf die Präventionspflichten des Herstellers: Eine Maßnahme zur Vermeidung von Rechtsgutsverletzungen genügt nur dann

---

[23] *Oster*, in: Foerste/Graf v. Westphalen (Hrsg.), Produkthaftungshandbuch, § 57 Rn. 25.

[24] Anders aber *Rockstroh/Kunkel*, MMR 2017, 77 (81); *Spindler*, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, 63 (75); zurückhaltend auch *Foerste*, in: Foerste/Graf v. Westphalen (Hrsg.), Produkthaftungshandbuch, § 24 Rn. 363a.

[25] *Regenfus*, JZ 2018, 79 (83): Mit Hinweis in Fn. 41 auf die Boston-Scientific-Entscheidung des EuGH, in der die Deaktivierung des Geräts bzw. einer gefährlichen Funktion als grundsätzlich ausreichende Maßnahme der Gefahrenabwehr angesehen wurde, vgl. EuGH NJW 2015, 1163 (1164 f.); ähnlich *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, 232.

[26] *Regenfus*, JZ 2018, 79 (83); MüKoBGB/*Wagner*, § 823 Rn. 1133; *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (90).

[27] OLG Karlsruhe NJW 1996, 200 (201); *Riehm*, VersR 2019, 714 (717).

[28] Vgl. MüKoBGB/*Wagner*, § 823 Rn. 1133.

den Anforderungen des Produkthaftungsrechts, wenn sie auch praktisch wirksam ist.[29] Ist allerdings damit zu rechnen, dass die Nutzer ihre Einwilligung zu einer Maßnahme (z.B. der Totalabschaltung ihrer Geräte) nicht erteilen werden und besteht auch kein anderer Rechtfertigungsgrund, so ist diese Maßnahme auch nicht geeignet, um Rechtsgutsverletzungen durch das Produkt effektiv zu verhindern.

Verweigert der Nutzer seine Einwilligung, kommt zwar eine Rechtfertigung des Herstellers unter dem Gesichtspunkt des Defensivnotstands nach § 228 S. 1 BGB in Betracht.[30] Allerdings gilt es hier zu berücksichtigen, dass nach dem Grundsatz des geringsten Eingriffs nur das mildeste der zur Verfügung stehenden geeigneten Mittel eingesetzt werden darf.[31] Weniger eingriffsintensiv als die Deaktivierung des Gerätes ist zunächst die zwangsweise, d.h. die ohne Zustimmung des Nutzers durchgeführte Aktualisierung durch den Hersteller. Gleiches gilt für die bloße Bereitstellung einer Aktualisierung, auf die der Nutzer hingewiesen wird und die er eigenverantwortlich herunterladen sowie installieren kann. Nachdem im Rahmen des Defensivnotstands zunächst grundsätzlich weniger eingriffsintensive Abwehrmittel genutzt werden müssen, selbst wenn deren Wirkung nicht völlig sicher ist,[32] stellt die bloße Bereitstellung einer Aktualisierung somit eine „Grundmaßnahme" dar. Nur wenn der Nutzer einer Aktualisierungsaufforderung nicht nachkommt, diese von vorneherein keinen Erfolg verspricht oder die zeitnahe Verwirklichung der Gefahr ein Zuwarten nicht zulässt, ist eine Zwangsaktualisierung oder -deaktivierung in Betracht zu ziehen.[33] Insoweit ergibt sich ein „Stufenbau der Reaktionspflichten",[34] sodass die Bereitstellung von Softwareaktualisierungen zunächst das Mittel der Wahl darstellt, um den Anforderungen des Produkthaftungsrechts zu genügen.

III. Kein vorbeugender gesetzlicher Anspruch auf Aktualisierungen

Unklar ist schließlich, ob und ggf. unter welchen Voraussetzungen im Einzelnen eine derartige Aktualisierungspflicht, die im Kern eine rein präventiv wirkende deliktische Verkehrspflicht ist, durch einen vorbeugenden Anspruch auf Sicherheitsaktualisierungen durchgesetzt werden kann. Im Regelfall werden deliktische Verkehrspflichten erst *ex post* relevant, wenn ein Schaden bereits eingetreten ist und sich die Frage stellt, ob dieser auf einer verkehrspflichtwidrigen Handlung eines Schädigers beruht. Eine unmittelbare Durchsetzung von Verkehrspflichten wird sich allenfalls auf der Grundlage

[29] BGH NJW 2009, 1080 (1082).

[30] *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (91); *Regenfus*, JZ 2018, 79 (85).

[31] Vgl. nur MüKoBGB/*Grothe*, § 228 Rn. 9; BeckOK BGB/*Dennhardt* § 228 Rn. 8; BeckOGK BGB/*Rövekamp*, 01.12.2023, § 228 Rn. 20.

[32] BeckOGK BGB/*Rövekamp*, § 228 Rn. 21; MüKoBGB/*Grothe*, § 228 Rn. 9.

[33] *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, 102 f.; MüKoBGB/*Wagner*, § 823 Rn. 1033.

[34] *Sommer*, Haftung für autonome Systeme, 284.

von § 1004 I BGB begründen lassen.[35] Dieser Anspruch ist auf die Beseitigung einer konkreten Gefahr gerichtet. In den Fällen aber, in denen der Nutzer in der Lage ist, einen Gefahrenabwehranspruch hinreichend konkret zu formulieren und zu begründen (§ 253 II Nr. 2 ZPO), wird die Kenntnis der Gefahr regelmäßig auch für die Ergreifung von Selbstschutzmaßnahmen ausreichen.[36] Insoweit kann niemand von einem Hersteller mit der Begründung eine Softwareaktualisierung verlangen, dass andernfalls die Warnung ignoriert und das Produkt trotz der erkannten Gefahr weiter verwendet werde.[37] Dieser einfache und zumutbare Selbstschutz wird Dritten, die zufällig mit dem gefährlichen Produkt in Kontakt kommen, zwar nicht möglich sein. Allerdings fehlt es in diesen Fällen regelmäßig an der hinreichenden Konkretisierung der Gefahr, sodass auch Ansprüche Dritter auf Vornahme von Sicherheitsaktualisierungen zumindest aus praktischen Gründen ausscheiden.[38]

B. Vertragliche Ansprüche im B2C-Verhältnis (§§ 327 ff., 475b ff. BGB)

Im Mittelpunkt dieses Beitrags stehen vertragliche Ansprüche auf Sicherheitsaktualisierungen im B2C-Verhältnis. Hier besteht, wie eingangs ausgeführt, seit dem 01.01.2022 eine explizite gesetzliche Regelung von Aktualisierungspflichten. Im Hinblick auf Verträge über digitale Produkte sieht § 327f I BGB vor, dass der Unternehmer sicherzustellen hat, „dass dem Verbraucher während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert wird. Zu den erforderlichen Aktualisierungen gehören auch Sicherheitsaktualisierungen." Diese Vorschrift gilt für Verträge über die Bereitstellung von digitalen Inhalten und Dienstleistungen, also auch für jegliche Art von Software. Sie ist zudem unabhängig vom Vertragstyp anwendbar und gilt sowohl für Verträge über die „dauerhafte Bereitstellung" („Mietmodell") als auch für Verträge über die „einmalige Bereitstellung" („Kaufmodell"). Im Hinblick auf die Aktualisierungspflicht unterscheiden sich beide Modelle lediglich im „maßgeblichen Zeitraum" (§ 327f I 3 BGB), während dessen die Sicherheitsaktualisierungen bereitzustellen sind. Beim Mietmodell ist dies der gesamte Zeitraum, über den das digitale Produkt selbst bereitzustellen ist, also die Vertragslauf-

[35] Grundlegend zur Aufwertung von Verkehrspflichten hin zu selbständig einklagbaren Pflichten *v. Bar*, in: 25 Jahre Karlsruher Forum, 1983, 80 ff.; vgl. auch MüKoBGB/*Wagner*, Vor § 823 Rn. 44.

[36] *Bodewig*, Der Rückruf fehlerhafter Produkte, 1999, 364.

[37] MüKoBGB/*Wagner*, § 823 Rn. 1128; *Raue*, NJW 2017, 1841 (1845).

[38] *Raue*, NJW 2017, 1841 (1845).

zeit (Bereitstellungszeitraum, § 327e I 3 BGB), während es beim Kaufmodell der Zeitraum ist, „den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann".

Parallel hierzu regelt § 475b IV Nr. 2 BGB ebenfalls eine Aktualisierungspflicht im Rahmen von Kaufverträgen über „Waren mit digitalen Elementen". Dabei handelt es sich um Waren, „die in einer Weise digitale Produkte enthalten oder mit ihnen verbunden sind, dass die Waren ihre Funktionen ohne diese digitalen Produkte nicht erfüllen können" (§ 327a III 1 BGB). Mit anderen Worten ist die Vorschrift auf physische Waren mit einer betriebsnotwendigen Software anzuwenden (Paradigma *embedded software)*. Beide Regelungen sind hinsichtlich des Inhalts der Aktualisierungspflicht und ihrer Dauer im Wesentlichen parallel konstruiert.

I. Sicherheitsanforderungen für digitale Produkte

Gemeinsame Voraussetzung der genannten Vorschriften ist die Erforderlichkeit der Aktualisierungen zum Erhalt der Vertragsmäßigkeit des digitalen Produkts im Hinblick auf die Sicherheit. Schon ab Vertragsschluss und unabhängig von der Aktualisierungspflicht besteht zudem die Pflicht, das Produkt im vertragsgemäßen Zustand bereitzustellen (§§ 327d, 433 I 2 BGB). In der Summe besteht unter beiden Gesichtspunkten eine vertragliche Pflicht zur Einhaltung von Sicherheitsanforderungen als Element der objektiven Sollbeschaffenheit.

1. „Sicherheit" als Element der objektiven Beschaffenheit

Sowohl im Hinblick auf digitale Produkte als auch auf Waren mit digitalen Elementen bezieht sich der objektive Mangelbegriff im Rahmen der „üblichen und erwartbaren Beschaffenheit" auch auf die „Sicherheit" (§§ 327e III 1 Nr. 2, 434 III 2 BGB). Der nationale Gesetzgeber spezifiziert allerdings nicht näher, was mit dem Begriff der Sicherheit gemeint ist. Unklar ist, ob sowohl *safety* (=Betriebssicherheit) als auch *security* (=Informationssicherheit) umfasst sind.[39]
Die englische Sprachfassung (*security)* der den §§ 327e bzw. 434, 475b BGB zugrundeliegenden Richtlinien legt nahe, dass mit Sicherheit in erster Linie die Informationssicherheit gemeint ist. Im Kommissionsentwurf zur Digitale-Inhalte-Richtlinie[40] war die Stärkung der Informationssicherheit in Erwägungsgrund 27 S. 3 auch noch explizit als „vorrangiges Anliegen" adressiert. Dass der europäische Gesetzgeber hier Handlungs-

[39] Zu den Begriffen *safety* und *security* bereits unter A.I.

[40] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 9.12.2015 (COM(2015) 634 final).

bedarf erkannte, erscheint vor dem Hintergrund einer kontinuierlich wachsenden Bedrohungslage verständlich. Hieraus sollte jedoch keine Beschränkung auf die *security* geschlussfolgert werden.[41] Wie bereits oben unter A.I. ausgeführt, lassen sich *security* und *safety* im Hinblick auf Software nicht trennen – auch und gerade nicht im Hinblick auf IoT-Geräte. Die Herausstellung der Informationssicherheit als Qualitätsmerkmal erklärt sich vielmehr damit, dass sich *security*-Defizite regelmäßig nur materialisieren, wenn ein vorsätzlich handelnder Dritter dazwischentritt. Das Erfordernis der Betriebssicherheit von Produkten ergibt sich dagegen bereits aus der Sache selbst und war auch vor den Richtlinien bereits als Qualitätsmerkmal anerkannt.[42]
Damit umfasst der Begriff der Sicherheit in §§ 327e, 434 BGB einerseits die Sicherheit gegenüber (zu erwartenden) Angriffen böswilliger Dritter: Der Nutzer muss sich darauf verlassen können, dass das von ihm erworbene Produkt gegen Angriffe von außen hinreichend geschützt ist, weil gerade solche Angriffe die Nutzbarkeit erheblich einschränken, oder sogar ausschließen können. Andererseits müssen Produkte betriebssicher, also *safe*, sein. Sie dürfen sowohl bei ordnungsgemäßer Bedienung als auch bei naheliegenden Fehlbedienungen keine Gefahren für bestehende Rechtsgüter hervorrufen. Das gilt ohne weiteres auch für Software.

2. Geschuldeter Sicherheitsstandard

Zu bestimmen ist jedoch, welches Maß an Sicherheit von Software geschuldet ist. Dies ist besonders problematisch vor dem Hintergrund des Umstands, dass aus technischer Sicht komplexe Software niemals 100 % fehlerfrei sein kann.[43]

a) Subjektive Anforderungen

Zunächst können subjektive Anforderungen im Hinblick auf die Sicherheit der Software vertraglich vereinbart werden. Zwar ist die Sicherheit nicht ausdrücklich als Beispiel für subjektive Anforderungen in den §§ 327e II 1 Nr. 1a, 434 II 1 Nr. 1 BGB erwähnt; es spricht aber nichts dagegen, diese gleichwohl als Element der Beschaffenheit zu verstehen, über welches die Parteien ausdrückliche Vereinbarungen treffen können. Freilich werden solche individuellen Beschaffenheitsvereinbarungen im B2C-Kontext kaum je vorkommen.[44] Denkbar sind sie etwa, wenn der Verkäufer jenseits allgemeiner

[41] *Schmidt-Kessel*, ZfPC 2022, 117 (118 f.); *Martens*, Schuldrechtsdigitalisierung, 2022, Rn. 80; *Gelbrich/Timmermann*, NJOZ 2021, 1249 (1252); a.A. Staudinger BGB/*Heinze*, Neubearb. 2023, § 327e Rn. 51; MüKoBGB/*Metzger*, 9. Aufl. 2022, § 327e Rn. 38.

[42] BGH NJW 1985 1769 (1770); MüKoBGB/*Westermann*, 8. Aufl. 2019, § 434 Rn. 73.

[43] Dazu grundlegend bereits *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, 37 ff.; *Hohler*, in: Pfeifer/Schmitt/Masing (Hrsg.), Masing Handbuch Qualitätsmanagement, 7. Aufl. 2021, 425 (430).

[44] *Kipker/Walkusz*, RDi 2021, 30 (31); *Söbbing*, ITRB 2020, 12 (13).

Werbeangaben[45] bestimmte IT-Sicherheitszertifizierungen (bspw. nach *Common Criteria*) verspricht.

Im Hinblick auf das Erfordernis einer Eignung der Software zur nach dem Vertrag vorausgesetzten Verwendung (§§ 327e II 1 Nr. 1b, 434 II 1 Nr. 2 BGB) kommen subjektive Anforderungen ebenfalls in Betracht. Auch hier bleibt fraglich, inwieweit spezifische Verwendungszwecke tatsächlich im B2C-Kontext individualvertraglich vereinbart werden. Denkbar ist das etwa, wenn der Verbraucher für den Unternehmer erkennbar beabsichtigt, personenbezogene Daten Dritter zu verarbeiten, was gem. Art. 32 DSGVO die Einhaltung eines angemessenen Sicherheitsniveaus erfordert.[46]

Insgesamt dürfte die praktische Bedeutung subjektiver Anforderungen an die Sicherheit digitaler Produkte und an Waren mit digitalen Elementen im Verbraucherkontext aber gering sein.

b) Objektive Sicherheitsanforderungen

Die objektiven Beschaffenheitsanforderungen nach §§ 327e III, 434 III BGB beziehen sich gegenständlich ausdrücklich auch auf die Sicherheit. Maßstab ist insoweit zum einen die übliche und erwartbare Beschaffenheit, zum anderen die Eignung für die gewöhnliche Verwendung. Von den objektiven Anforderungen kann im B2C-Verkehr nur unter den hohen Hürden der §§ 327h, 476 I 2 BGB zu Lasten der Verbraucher[47] abgewichen werden.[48] Mit der Einführung dieser Vorgaben wurde die Bedeutung der objektiven Kriterien enorm aufgewertet.

aa) Fehlen jeglicher Sicherheitslücken als berechtigterweise erwartbare Beschaffenheit

Vor dem Hintergrund, dass komplexe Software faktisch niemals zu 100 % fehlerfrei sein kann, und auch die Produkte großer und anerkannter Softwareanbieter (bisweilen gravierende) Sicherheitslücken aufweisen, wird man das Fehlen von Sicherheitslücken statistisch wohl nicht als „übliche Beschaffenheit" von Software bezeichnen können. Dies führt jedoch nicht dazu, dass die objektiven Beschaffenheitsanforderungen entsprechend zu reduzieren wären. Denn die nach §§ 327e III 1, 434 III 1 BGB geschuldete Beschaffenheit ergibt sich nicht nur aus der „üblichen Beschaffenheit" und der „Eignung

[45] Diese ordnen die §§ 327e III 2, 434 III 1 Nr. 2b BGB der objektiven Beschaffenheit zu.

[46] *Eichfeld*, Die Haftung des Verkäufers für fehlende Datenschutzkonformität von „Waren mit digitalen Elementen", 2022, 241 f.

[47] Zur Beschränkung auf negative Abweichungen *Rachlitz/Kochendörfer/Gansmeier*, JZ 2022, 705 (709).

[48] Kritisch zu der praktischen Umsetzbarkeit der Vorgaben bereits *Riehm/Abold*, CR 2021, 530 (534 f.).

für die gewöhnliche Verwendung" als dem tatsächlich *üblichen* Marktstandard, sondern zudem aus der „berechtigten Käufererwartung" als einem *normativen* Standard.[49] Dabei handelt es sich um ein eigenständiges Merkmal, das ein bestehendes Marktversagen korrigieren kann, wenn das marktübliche Beschaffenheitsniveau unzureichend ist. Angesichts der faktischen Verbreitung von Sicherheitslücken trotz ihrer objektiven Gefährlichkeit und Beeinträchtigung der vertragsgemäßen Nutzung wird man ein solches Marktversagen im Hinblick auf die IT-Sicherheit von Softwareprodukten bejahen müssen.[50]

Eine Software, die eine Sicherheitslücke hat – unabhängig davon, ob diese bereits entdeckt wurde oder entdeckbar war –, entspricht nicht der berechtigten Käufererwartung, (wenn und) weil ihr Einsatz mit Gefahren für die digitale Infrastruktur des Nutzers und/oder für Dritte verbunden ist (§ 2 VI BSIG, s.o. A.I.). Ein verständiger Verbraucher muss aber nicht erwarten, dass die von ihm eingesetzte Software eine Sicherheitslücke beinhaltet, deren Ausnutzung zu Einschränkungen der Nutzbarkeit der Software selbst oder zur Verletzung sonstiger Rechte und Rechtsgüter führen kann. Das gilt selbst, solange die Sicherheitslücke noch unbekannt ist, besteht doch auch in diesen Fällen das latente Risiko eines Zero-Day-Exploits. Dem Verbraucher muss, jedenfalls während der Gewährleistungsfrist, ein Anspruch auf Bereitstellung einer Sicherheitsaktualisierung im Wege der Nacherfüllung zustehen. Das setzt aber die Annahme eines Mangels voraus. Unter diesem Gesichtspunkt kann tatsächlich jede Sicherheitslücke als Verstoß gegen die objektiven Beschaffenheitsanforderungen im Hinblick auf die Sicherheit angesehen werden. Auf die Erkennbarkeit der Lücke für den Unternehmer oder gar dessen Kenntnis von ihr kommt es im Rahmen der objektiven Beschaffenheitsanforderungen nicht an. Diese spielen nur bei verschuldensabhängigen Rechtsbehelfen (Schadensersatz, s.u.B.III.3.) eine Rolle.

Gegen diese strenge Interpretation der Sicherheitsanforderungen wird teilweise eingewandt, sie seien unmöglich zu erfüllen (§ 275 I BGB).[51] Indessen würde selbst das nichts an der Wirksamkeit des entsprechenden Vertrags ändern, denn § 311a I BGB sieht ausdrücklich vor, dass Verträge sogar über unmögliche Leistungen wirksam abge-

[49] Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, 2020, Art. 8 DCD Rn. 36, 58; Staudinger BGB/*Heinze*, § 327e Rn. 56; HK-BGB/*Schulze*, 11. Aufl. 2021, § 327e BGB Rn. 23; ebenso MüKoBGB/*Metzger*, § 327e Rn. 31, 42, der aber eine Diskrepanz der beiden Merkmale nur bei öffentlichen Äußerungen bejaht; a.A. Staudinger BGB/*Matusche-Beckmann*, Neubearb. 2023, § 434 Rn. 112.

[50] *European Commission* (Hrsg.), Study on the need of Cybersecurity requirements for ICT products, 2021 (https://ec.europa.eu/newsroom/dae/redirection/document/82006), 69 (geprüft am 15.03.2024); *bitkom*, Zur Sicherheit softwarebasierter Produkte, 2016 (https://bitkom.org/sites/default/files/file/import/160920-Sicherheit-softwarebasierte-Produkte-final.pdf), 8 (geprüft am 15.03.2024).

[51] In diese Richtung *Pour Rafsendjani/Bomhard*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, § 9 Rn. 13, 15, 135.

schlossen werden können; das gilt auch im Hinblick auf die geschuldete Beschaffenheit.[52] Im Hinblick auf konkrete Sicherheitslücken stellt sich nach ihrer Entdeckung die Frage der Unmöglichkeit ihrer Beseitigung im Wege der Nacherfüllung bzw. durch Softwareaktualisierung in der Regel ohnehin nicht mehr. Die „Unmöglichkeit" der Fehlerfreiheit ist mit anderen Worten nur eine abstrakte Feststellung, die konkreten Rechten aus einzelnen Fehlern nicht entgegensteht.

bb) Jedenfalls: Einhaltung des Stands der Technik bei der Softwareentwicklung geschuldet

Zudem kommt die Annahme der Unmöglichkeit einer mangelfreien Leistung ohnehin nur in seltenen Fällen in Betracht: Unmöglichkeit von 100 % Fehlerfreiheit ist zunächst eine technische Kategorie, die sich auf alle Arten von Softwarefehlern im technischen Sinne bezieht. Nur ein kleiner Bruchteil dieser möglichen Fehler ist überhaupt sicherheitsrelevant.[53] Die meisten Sicherheitslücken gehen auf die Verwendung veralteter Fremdkomponenten wie Bibliotheken[54] oder auf die Missachtung elementarer Programmier- oder Teststandards zurück.[55] Vor diesem Hintergrund sollte der Diskussion um eine Unmöglichkeit der Fehlerfreiheit nicht allzu viel Gewicht beigemessen werden.

Selbst wenn man der vorstehenden Argumentation nicht folgen sollte, ist jedenfalls die Einhaltung des Stands der Technik in Bezug auf sichere Softwareentwicklung als berechtigterweise erwartbare Beschaffenheit geschuldet.[56] Das erfordert, dass beim Pla-

---

[52] MüKoBGB/*Ernst*, § 311a Rn. 80; BGH NJW 2005, 2852 (2854).

[53] *Redeker*, IT-Recht, 8. Aufl. 2023, Rn. 335; *Deusch/Eggendorfer*, K&R 2016, 152 (152 f.).

[54] *Bundesamt für Sicherheit in der Informationstechnik* (BSI), Die Lage der IT-Sicherheit in Deutschland, 2023 (https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf), 35 (geprüft am 15.03.2024); *Microsoft*, Microsoft Digital Defense Report, 2022 (https://microsoft.com/de-de/security/business/microsoft-digital-defense-report-2022), 66 (geprüft am 15.03.2024).

[55] *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-HdB, 50.1 Rn. 452; *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, 165; *Sohr/Kemmerich*, in: Kipker (Hrsg.), Cybersecurity, Kap. 3 Rn. 192.

[56] *Gomille*, Der Feind in meinem Haus, 2023 (https://irdt.uni-trier.de/wp-content/uploads/2023/05/GOMILLE_IRDT_7.2.2023_Manuskript.pdf), 11 f. (geprüft am 15.03.2024); *Söbbing*, ITRB 2020, 12 (14); *B.A. Koch*, FS Eccher, 2017, 551 (564); ähnlich MüKoBGB/*Metzger*, § 327e Rn. 38; a.A. *Peschel/Rockstroh*, NJW 2020, 3345 (3347); *Kipker/Walkusz*, RDi 2021, 30 (32); *Gaden*, in: Kipker (Hrsg.), Cybersecurity, Kap. 20.3 Rn. 25, die eine Anknüpfung an den Stand der Technik für zu streng halten; anders ebenso *Voigt*, in: Frenz (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, 2020, 201 (205): Mangel nur bei „besonders gravierender Sicherheitslücke"; ähnlich: *Braun*, CR 2022, 727 (730), wonach kein Mangel vorliegen soll, wenn eine Lücke „praktisch kaum ausnutzbar ist und die sonstige Funktionsfähigkeit nicht beeinträchtigt".

nen, Programmieren sowie Testen der Software solche Methoden und Werkzeuge eingesetzt wurden, die dem *state of the art* entsprechen.[57] Enthält das Produkt eine Sicherheitslücke, die bei Einhaltung dieses (prozessbezogenen) Stands der Technik entdeckt bzw. vermieden worden wäre, entspricht es nicht der erwartbaren Beschaffenheit.

cc) Zusätzliche Anforderung: Updatability

Als weitere Minimalanforderung im Hinblick auf die Softwaresicherheit ist die „Updatability" anzusehen, d.h. die Fähigkeit von Geräten, die Software beinhalten, aktualisiert zu werden. Hierfür wird im Regelfall – jedenfalls bei Software, die auf Geräten mit Netzwerkanbindung eingesetzt werden soll – erforderlich sein, dass das betroffene Gerät über eine Schnittstelle verfügt, über die Aktualisierungen eingespielt werden können.

dd) Fazit

Insgesamt liegt ein Sicherheitsmangel daher jedenfalls vor, wenn die Software gemäß dem Stand der Technik nicht sicher entwickelt wurde, also insbesondere eine durch ordnungsgemäße Softwareentwicklung vermeidbare Sicherheitslücke enthält. Darüber hinaus entspricht eine Software nach hier vertretener Auffassung nur dann den objektiven Anforderungen im Sinne der erwartbaren Beschaffenheit, wenn sie überhaupt keine Sicherheitslücken enthält – d.h. auch keine Sicherheitslücken, die bei einer Softwareentwicklung nach dem Stand der Technik unvermeidbar gewesen wären.

c) Relevanter Zeitpunkt für die Einhaltung der Sicherheitsanforderungen

Grundsätzlich ist im Kaufrecht sowie im Kaufmodell bei Verträgen über digitale Produkte die Einhaltung der Beschaffenheitsanforderungen nur im Zeitpunkt des Gefahrübergangs bzw. der Bereitstellung geschuldet (§§ 434 I, 327e I 2 BGB).[58] Software darf keine Eigenschaften aufweisen, die in diesem Zeitpunkt als Sicherheitslücke anzusehen

[57] *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-HdB, 50.1 Rn. 452.

[58] Zwar werden die Beschaffenheitsanforderungen selbst im Vertrag festgelegt und richten sich deshalb regelmäßig nach der Kenntnislage zu diesem Zeitpunkt (BeckOK BGB/*Faust*, § 434 Rn. 26, 83; *Rieländer*, GPR 2021, 257 (266)). Aufgrund der mit Sicherheitslücken einhergehenden Risiken widerspräche es jedoch den berechtigten Parteiinteressen für die Festlegung konkreter Sicherheitsanforderungen auf den Zeitpunkt des Vertragsschlusses abzustellen. Stattdessen richten sie sich nach dem Kenntnisstand zum Zeitpunkt des Gefahrübergangs bzw. der Bereitstellung. So auch für die Einhaltung technischer Normen Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 24; Staudinger/*Heinze* § 327e Rn. 45.

sind, weil bekannte Angriffsmethoden sie ausnutzen können.[59] Dies gilt auch weiterhin für Konstellationen, in denen keine Aktualisierungspflicht besteht.[60]

Für den B2C-Verkehr geht aus der Formulierung der Vorschriften über die Aktualisierungspflichten (§§ 327f I 1, 475b IV Nr. 2 BGB) aber hervor, dass die Aktualisierungen dem Erhalt der Vertragsmäßigkeit „während des maßgeblichen Zeitraums" dienen sollen. Hieraus folgt, dass – abweichend vom allgemeinen Kaufrecht – die vertragskonforme Beschaffenheit während des gesamten „maßgeblichen Zeitraums" erhalten werden muss. Das ist der Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann (§§ 327f I 3 Nr. 2, 475b IV Nr. 2 BGB). Das klassisch nur auf einen punktuellen Leistungsaustausch ausgerichtete Pflichtenprogramm des Kaufvertrags erhält hierdurch eine Dauerschuldkomponente.[61]

Wenn während des Aktualisierungszeitraums die Vertragsmäßigkeit zu erhalten ist, bedeutet das zunächst unzweifelhaft, dass die bei Bereitstellung geltenden Beschaffenheitsanforderungen im Hinblick auf die Sicherheit[62] während des gesamten Zeitraums eingehalten und – sollten sie anfänglich fehlen – ggf. im Wege der Nacherfüllung herbeigeführt werden müssen. Vergegenwärtigt man sich, dass die Aktualisierungspflicht die langfristige Nutzbarkeit der Software trotz veränderter Umweltvariablen sicherstellen soll,[63] erfordert der Erhalt der Vertragsmäßigkeit darüber hinaus aber auch, dass Weiterentwicklungen der Sicherheitsanforderungen während des Aktualisierungszeitraums berücksichtigt werden.[64] Das bedeutet, dass Aktualisierungen auch dann erforderlich sind, wenn ein Softwarezustand, der sich bei der Bereitstellung als vertragsgemäß darstellt, später vertragswidrig wird, etwa weil neue Angriffsmethoden entwickelt

---

[59] *Mankowski*, in: Ernst (Hrsg.), Hacker, Cracker & Computerviren, 2004, Kap. 3 Rn. 456; *Raue*, NJW 2017, 1841 (1843); *Lapp*, in: Kipker (Hrsg.), Cybersecurity, Kap. 10 Rn. 119; *Burrer*, in: Bräutigam/Kraul/Bauer (Hrsg.), Internet of Things, 2021, § 8 Rn. 38; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 132; *Hoffmann/Löffler*, ZfPW 2023, 1 (8); *Marly*, Praxishandbuch Softwarerecht, 7. Aufl. 2018, Rn. 1528; Schuster/Grützmacher/*Diedrich*, IT-Recht, 2020, § 434 BGB Rn. 65; *Wiegand*, in: Kipker (Hrsg.), Cybersecurity, Kap. 9 Rn. 53.

[60] B2B-, C2C- und C2B-Verkehr sowie Fälle, in denen die Aktualisierungspflicht gem. §§ 327h, 476 I 2 BGB wirksam abbedungen wurde.

[61] Insofern bereits zur Allgemeinen Ausrichtung des Rates zur DIDRL *Riehm/Abold*, ZUM 2018, 82 (87).

[62] Dazu eingehend oben unter B.I.1.

[63] ErwG 47 S. 1 DIDRL, ErwG 31 S. 1 u. 2 WKRL.

[64] *Kroschwald/Polenz*, in: Brönneke/Föhlisch/Tonner (Hrsg.), Das neue Schuldrecht, 2022, § 6 Rn. 92; *Voigt*, IT-Sicherheitsrecht, Rn. 132; *Hoffmann/Löffler*, ZfPW 2023, 1 (7 f.); *Eichfeld*, Die Haftung des Verkäufers für fehlende Datenschutzkonformität von „Waren mit digitalen Elementen", 266; so auch die Gesetzesbegründung, wonach die Aktualisierungspflicht gerade der Wahrung des Stands der Technik dient: Entwurf eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags vom 09.03.2021, 33 (BT-Drucksache 19/27424); ; insgesamt zur Dynamisierung der Qualitätsanforderungen durch die Aktualisierungspflicht: *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, 2023, 19 f.; *Poneder*, JBl 2024, 10 (16 f.); a.A. *Braun*, CR 2022, 727 (728): „neue Sicherheitsfeatures werden nicht geschuldet".

wurden, die bei Bereitstellung noch nicht denkbar waren – z.B. durch neue kryptographische Methoden, die eine zunächst sichere Verschlüsselung nunmehr angreifbar machen. Die Entwicklung der IT-Sicherheitsanforderungen an Produkte (wegen fortentwickelter Angriffs- wie Verteidigungsmöglichkeiten) führt so zu einer Dynamisierung der sicherheitsbezogenen Beschaffenheitsanforderungen, die Aktualisierungspflichten auslösen. Die Software ist daher im Rahmen der Aktualisierungspflichten während des gesamten Aktualisierungszeitraums an *evolvierende* Sicherheitsanforderungen anzupassen.

Für eine solche Dynamisierung der Qualitätsanforderungen spricht v.a. die gesetzgeberische Zielsetzung, die mit den Aktualisierungspflichten verfolgt wird, nämlich die Förderung der IT-Sicherheit von digitalen Verbraucherprodukten.[65] Dieser wäre nur beschränkt gedient, wenn Anbieter nicht auch verpflichtet wären, ihre digitalen Produkte an neuartige Angriffsvektoren anzupassen. Wären die Aktualisierungspflichten nur darauf gerichtet, die Software gegen potenzielle Sicherheitsbedrohungen zum Bereitstellungszeitpunkt abzusichern, hätten sie gegenüber dem ohnehin bestehenden Nacherfüllungsanspruch für anfängliche Sicherheitsmängel keine zusätzliche Funktion außer ggf. der Verlängerung des Aktualisierungszeitraums über die Verjährungsfrist für den Nacherfüllungsanspruch hinaus. Eine eigenständige Bedeutung und Funktion für die Gewährleistung von IT-Sicherheit erhalten sie erst dadurch, dass durch sie effektiv sichergestellt werden kann, dass von den digitalen Produkten während des Aktualisierungszeitraums keine Gefahren für die IT-Sicherheit ausgehen. Das ist aber nur der Fall, wenn sie darauf gerichtet sind, die Produkte an *evolvierende* Sicherheitsanforderungen anzupassen. Weder dem Interesse der Verbraucher an sicher nutzbarer Software noch dem gesamtgesellschaftlichen Interesse an sicherer IT-Infrastruktur wäre gedient, wenn Anbieter sich während des gesetzlichen Aktualisierungszeitraums darauf berufen könnten, dass die Software (lediglich) im Zeitpunkt der Bereitstellung sicher war, wenn sie es nun nicht mehr ist. Eine Differenzierung zwischen Mietmodell und Kaufmodell ist angesichts der gesetzgeberischen Gleichbehandlung beider (mit Ausnahme der Dauer des Aktualisierungszeitraums) insoweit ebenfalls nicht angezeigt.

[65] Das zeigt bereits die exponierte Position von Sicherheitsupdates in § 327f I 2 BGB; zur Rolle von Sicherheitsupdates bei der Schaffung der Aktualisierungspflicht Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 116; *Janssen*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Smart Products, 2022, 91 (96); auch nach ErwG 47 S. 1 DIDRL sollen die Aktualisierungen sicherstellen, dass das digitale Produkt „sicher bleibt" (engl. „keep the digital content or digital service secure").

II. Ansprüche auf Beseitigung von Sicherheitsmängeln

Aus einer bloßen Beschaffenheitsanforderung folgt aber nicht automatisch auch ein durchsetzbarer Anspruch des Verbrauchers gegen seinen Vertragspartner auf Beseitigung von Sicherheitsmängeln, d.h. auf die Bereitstellung von Sicherheitsaktualisierungen. Insoweit ist hinsichtlich der dogmatischen Konstruktion zwischen dem Mietmodell und dem Kaufmodell zu unterscheiden.

1. „Mietmodell"

Im Mietmodell ergibt sich ohne weiteres, dass die Anforderungen an die Sicherheit während der gesamten Vertragslaufzeit eingehalten werden müssen (§§ 327e I 3, 475c II BGB). Sobald sich die Software nach den vorstehend geschilderten Anforderungen an ihre Sicherheit als vertragswidrig erweist, steht dem Verbraucher ein Anspruch auf Nacherfüllung zur Wiederherstellung der vertraglich geschuldeten Beschaffenheit zu (§§ 327l I 1, 439 I BGB). Dies gilt unabhängig von der ebenfalls bestehenden Pflicht des Unternehmers, die Versorgung mit Sicherheitsaktualisierungen sicherzustellen (§§ 327f I, 475b IV Nr. 2 BGB). Die Aktualisierungspflicht konkretisiert die allgemeine Erhaltungspflicht zunächst im Hinblick auf die geschuldete Leistung des Vermieters.[66] So muss der Unternehmer den vertragsgemäßen Zustand der vermieteten Software nicht unmittelbar selbst herbeiführen, wozu er ohnehin nur in der Lage ist, wenn er Zugriff auf das ausführende Gerät hat, sondern darf sich grundsätzlich darauf beschränken, Aktualisierungen bereitzustellen und über diese zu informieren (§§ 327f II, 475b V BGB).[67]

Zudem wird teilweise angenommen, die Aktualisierungspflicht gehe inhaltlich über die allgemeine Erhaltungspflicht hinaus.[68] Anders als die Erhaltungspflicht erstrecke sich die Aktualisierungspflicht auf nach Gefahrübergang bzw. Bereitstellung eintretende Entwicklungen der Sicherheitsanforderungen.[69] Dafür spricht zwar, dass der Aktualisierungspflicht bei Verträgen über die dauerhafte Bereitstellung sonst eine reine Konkretisierungsfunktion zukäme.[70] Da sich die Rechtsfolgen der Verletzung der Er-

---

[66] *Schmidt-Kessel*, in: Schmidt-Kessel/Kramme (Hrsg.), Handbuch Verbraucherrecht, 2023, Kap. 14 Rn. 123.

[67] BeckOK BGB/*Faust*, § 475b Rn. 34; *Leithäuser*, RDi 2023, 274 (278); *Möllnitz*, in: Schmidt-Kessel/Möllnitz (Hrsg.), Grundfragen des Digitalvertragsrechts, 2022, 17 (20).

[68] *Brießmann*, Die Bereitstellung digitaler Produkte i. S. v. § 327 Abs. 1 S. 1 BGB: vertragstypische Leistungspflicht?, 2023, 112; *Hubert/Hengstler*, MMR 2022, 623 (624); a.A. *Schmidt-Kessel*, in: Schmidt-Kessel/Kramme (Hrsg.), Handbuch Verbraucherrecht, Kap. 14 Rn. 123; *Martens*, Schuldrechtsdigitalisierung, Rn. 269, die eine Kongruenz von Aktualisierungspflicht und Erhaltungspflicht annehmen; in diese Richtung auch *Möllnitz*, in: Schmidt-Kessel/Möllnitz (Hrsg.), Grundfragen des Digitalvertragsrechts, 17 (18).

[69] Zur Erstreckung der Aktualisierungspflicht auf derartige Entwicklungen bereits unter B.I.2.c).

[70] *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, 102.

haltungspflicht einerseits sowie der Aktualisierungspflicht andererseits nicht unterscheiden[71] und beide Pflichten nur während der Vertragslaufzeit zu erfüllen sind, erscheint die Abgrenzung im Anwendungsbereich der §§ 327 ff., 475b ff. BGB jedoch müßig. Entscheidende Bedeutung erlangt die Abgrenzung bei Mietmodellen im B2B-Verkehr, bei denen es an einer Aktualisierungspflicht fehlt.[72] Im B2C-Verkehr ergibt sich ein Anspruch auf Sicherheitsaktualisierungen dagegen stets als Nacherfüllungsanspruch.

2. „Kaufmodell"

Überträgt man diesen Gedanken auf das Kaufmodell, so genügt ebenfalls der Nacherfüllungsanspruch (§§ 327l I, 439 I BGB), um vom Unternehmer die Beseitigung anfänglicher Sicherheitslücken zu verlangen. Das betrifft jedenfalls alle Sicherheitslücken, die im Zeitpunkt des Gefahrübergangs bzw. der Bereitstellung eine Abweichung von der oben (B.I.2.) beschriebenen Sollbeschaffenheit begründet haben (anfängliche Sicherheitsmängel), also auch Fälle, in denen anfängliche Sicherheitsmängel erst nachträglich entdeckt werden.

Die Pflicht zur Bereitstellung von Sicherheitsaktualisierungen aus §§ 327f I, 475b IV Nr. 2 BGB erlangt erst dann praktische Bedeutung, wenn Sicherheitsmängel nach Bereitstellung bzw. nach Gefahrübergang entstehen (nachträgliche Sicherheitsmängel) oder der Anspruch auf Nacherfüllung wegen anfänglicher Sicherheitsmängel bereits verjährt ist (§§ 327j I 1, 438 I Nr. 1, II BGB).[73] Ersteres kann etwa durch eine Weiterentwicklung der Sicherheitsanforderungen (s.o. B.I.2.c)) oder durch zwischenzeitlich eingespielte (andere) Softwareaktualisierungen geschehen, die ihrerseits eine neue Sicherheitslücke geschaffen haben, welche bei Bereitstellung bzw. Gefahrübergang noch nicht vorhanden war. Die genaue Rechtsnatur der Aktualisierungspflicht aus §§ 327f I, 475b IV Nr. 2 BGB ist dabei umstritten. Nach überwiegender und auch hier vertretener Auffassung begründet die Pflicht des Unternehmers, Sicherheitsaktualisierungen bereitzustellen, nicht selbst einen entsprechenden Anspruch des Verbrauchers, den dieser geltend machen könnte.[74] Vielmehr ordnet die gesetzliche Regelung

---

[71] Darauf verweisen auch *Brießmann*, Die Bereitstellung digitaler Produkte i. S. v. § 327 Abs. 1 S. 1 BGB: vertragstypische Leistungspflicht?, 112; MüKoBGB/*Metzger*, § 327f. Rn. 6; a.A. *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, 102 f.

[72] Dazu unter C.II.1.

[73] Dafür, dass die Aktualisierungspflicht auch zur Beseitigung anfänglicher Sicherheitsmängel verpflichtet, Staudinger BGB/*Heinze*, § 327f Rn. 18; a.A. Erman BGB/*Bernzen/Specht-Riemenschneider*, 17. Aufl. 2023, § 327f Rn. 11; *Martens*, Schuldrechtsdigitalisierung, Rn. 268, die von einer strengen Alternativität von anfänglichen Mängeln und Aktualisierungspflicht ausgehen.

[74] *Riehm/Abold*, CR 2021, 530 (538); *Schmidt-Kessel*, in: Schmidt-Kessel/Kramme (Hrsg.), Handbuch Verbraucherrecht, Kap. 14 Rn. 370; Staudinger BGB/*Heinze*, § 327f Rn. 10; *Staudinger/Artz*, Neues

die Aktualisierungspflicht der geschuldeten Sollbeschaffenheit zu (§§ 327e III 1 Nr. 5, 475b IV Nr. 2 BGB). Daraus folgt, dass das Ausbleiben einer geschuldeten Sicherheitsaktualisierung als Produktmangel bzw. Sachmangel einzuordnen ist und eine Verletzung der Aktualisierungspflicht die allgemeinen Gewährleistungsrechte auslöst. Ein Anspruch des Verbrauchers auf Bereitstellung der Sicherheitsaktualisierung ergibt sich dann auch in den Fällen der nachträglichen Sicherheitsmängel aus dem Nacherfüllungsanspruch (§§ 327l I, 439 I BGB).[75]

Wenig aussagekräftig ist die gesetzliche Regelung beim Kaufmodell bezüglich der Dauer, während derer die Sicherheitsaktualisierungen bereitgestellt werden müssen (§§ 327f I 3 Nr. 2, 475 IV Nr. 2 BGB). Die vage Formulierung „Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann" hilft bei der Suche nach einer konkreten Zeitspanne kaum weiter. Immerhin ist dem Erwägungsgrund 47 S. 2 der Digitale-Inhalte-Richtlinie zu entnehmen, dass der Unionsgesetzgeber von einer Mindestdauer von zwei Jahren ausgeht. Zudem hält der Gesetzgeber Differenzierungen zwischen der Dauer für Funktionsaktualisierungen einerseits und Sicherheitsaktualisierungen andererseits für möglich – hier entzündet sich der obige Streit (B.I.1.) um den Sicherheitsbegriff der Richtlinien.[76]

Insbesondere lässt es die gesetzliche Regelung nur unter den hohen Hürden der §§ 327h, 476 I 2 BGB zu, dass der Unternehmer den Aktualisierungszeitraum gegenüber den objektiven Anforderungen vertraglich begrenzt.[77] Einseitige Angaben in der Werbung des Unternehmers oder des Herstellers können zwar grundsätzlich eine berechtigte Verbrauchererwartung hinsichtlich inhaltlicher Beschaffenheitsanforderungen formen (§§ 327e III 2, 434 III 1 Nr. 2b BGB). Da das Produkt aber kumulativ der „erwartbaren" und der „üblichen" Beschaffenheit entsprechen muss (dazu bereits unter B.I.2.b)aa)), wirken sich Werbeaussagen praktisch nur aus, wenn sie über die übliche Beschaffenheit hinausgehen.[78] Werbeäußerungen können mithin nur das objektiv geschuldete Qualitätsniveau anheben, nicht aber absenken. Das wird man auf Äußerungen bezüglich Aktualisierungen übertragen können. Die Angaben des Herstellers können hinsichtlich des geschuldeten Aktualisierungszeitraums als zu berücksichtigende

Kaufrecht und Verträge über digitale Produkte, 2022, Rn. 154; a.A. *Felsch/Kremer/Wagener*, MMR 2022, 18 (21); *Hoffmann/Löffler*, ZfPW 2023, 1 (6); *Poneder*, JBl 2024, 10 (21).

[75] Näher *Leithäuser*, RDi 2023, 274 (276 ff.).

[76] *Rockstroh*, DuD 2023, 332 (333).

[77] *Wendehorst*, in: Stabentheiner/Wendehorst/Zöchling-Jud (Hrsg.), Das neue europäische Gewährleistungsrecht, 2019, 111 (134); Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 124; dagegen zweifelnd, ob eine vertragliche Verkürzung der Updatedauer auf weniger als zwei Jahre möglich ist: *Gaden*, in: Kipker (Hrsg.), Cybersecurity, Kap. 20.3 Rn. 48; *Reinking*, DAR 2021, 185 (190).

[78] BeckOK BGB/*Faust*, § 434 Rn. 106; so im Ergebnis auch Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 70; Problematisch ist insofern § 327e III 2 BGB, der vorgibt, die öffentlichen Äußerungen konkretisierten die übliche Beschaffenheit statt die berechtigte Verbrauchererwartung, ähnlich MüKoBGB/*Metzger*, § 327e Rn. 42.

„Umstände" für die objektive Bestimmung eine Rolle spielen, sofern sie über den branchenüblichen Zeitraum hinausgehen. Verkürzen können sie diesen Zeitraum nach der Wertung der §§ 327h, 476 I 2 BGB jedoch nicht.[79]

Perspektivisch wird der Cyber-Resilience-Act[80] eine Pflicht des Softwareherstellers begründen, den Verbraucher über den Zeitraum, während dessen er Sicherheitsaktualisierungen bereitstellen wird („Unterstützungszeitraum", Art. 3 Nr. 20 CRA), zu informieren (Art. 13 XIX UA 1, VIII UA 2 CRA). Dieser Zeitraum soll mindestens fünf Jahre betragen, sofern der Hersteller eine kürzere Erwartung nicht gesondert rechtfertigt (Art. 13 VIII UA 3 CRA). Auch Durchführungsmaßnahmen der bestehenden Ökodesign-RL und der kommenden Ökodesign-Verordnung drohen zeitliche Vorgaben bezüglich der Bereitstellung von Aktualisierungen aufzustellen.[81] Anders als der Cyber-Resilience-Act beschränken sich die Ökodesignanforderungen dabei nicht auf Sicherheitsaktualisierungen, sondern umfassen zur Vermeidung softwarebedingter Obsoleszenz auch Funktionsaktualisierungen.

Die hiernach geschuldeten Angaben und Zeiträume werden ebenfalls in die gerichtliche Bestimmung des geschuldeten Aktualisierungszeitraums einfließen können,[82] ohne diese allerdings abschließend einseitig zu determinieren. Vielmehr werden sie lediglich die Untergrenze der geschuldeten Aktualisierungsdauer festlegen, aber eine ggf. darüber hinausgehende gerichtliche Bestimmung des Zeitraums nicht verhindern können.

III. Folgen ausgebliebener Sicherheitsaktualisierungen

Ist der Unternehmer vertraglich verpflichtet, Sicherheitsaktualisierungen bereitzustellen, so stellt sich die Frage, welche Rechtsfolgen eintreten, wenn er dies pflichtwidrig unterlässt.

---

[79] So im Ergebnis auch Staudinger BGB/*Heinze*, § 327f Rn. 23; anders BT-Drucksache 19/27424, 33; Erman BGB/*Grunewald*, § 475b Rn. 4; *Sosnitza*, FS Becker-Eberhard, 2022, 535 (546), wonach öffentliche Äußerungen und Werbung insgesamt zur Bestimmung des Updatezeitraums einzubeziehen seien.

[80] Der Beitrag basiert auf dem am 12.03.2024 vom Europäischen Parlament beschlossenen Standpunkt im Hinblick auf den Erlass der Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2019/102, https://europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.pdf (geprüft am 15.03.2024).

[81] Beispielsweise jüngst hinsichtlich Smartphones und Tablets: Art. 3 i.V.m. Anhang 2 1.2 Nr. 6a der delegierten Verordnung (EU) 2023/1670 der Kommission vom 16.06.2023, wonach ab dem 20.06.2025 mindestens 5 Jahre lang Aktualisierungen für Betriebssysteme zugänglich gemacht werden müssen.

[82] Zum Einfluss der Ökodesign-Vorgaben auf die vertragliche Aktualisierungspflicht *Specht-Riemenschneider/Mehnert*, ZfDR 2022, 313 (332 ff.).

1. Nacherfüllungsanspruch auf Sicherheitsaktualisierungen

Wie vorstehend gezeigt, besteht der erste Rechtsbehelf des Verbrauchers im Anspruch auf Nacherfüllung (§§ 327l I, 439 I BGB), der auf die Bereitstellung von Sicherheitsaktualisierungen gerichtet sein kann. Das gilt sowohl für anfängliche als auch für nachträgliche Sicherheitsmängel, wobei bei den anfänglichen Sicherheitsmängeln die eigentliche Aktualisierungspflicht (§§ 327f, 475b IV Nr. 2 BGB) nach hier vertretener Auffassung praktisch nur eine Rolle spielt, wenn Ansprüche wegen anfänglicher Mängel verjährt sind (s.o. B.II.2.).

Problematisch ist insoweit, dass der Nacherfüllungsanspruch gegen den Vertragspartner des Verbrauchers (den Unternehmer) gerichtet ist, der keineswegs automatisch zugleich Hersteller der Software oder gar Hersteller derjenigen Softwarekomponente ist, die von der Sicherheitslücke betroffen ist. Rein praktisch wird der Unternehmer daher häufig nicht in der Lage sein, selbst Sicherheitsaktualisierungen bereitzustellen. Das führt jedoch regelmäßig nicht dazu, dass der Nacherfüllungsanspruch im Hinblick auf die Sicherheitsaktualisierungen am Einwand der subjektiven Unmöglichkeit (§§ 327 II 1 Alt. 1, 275 I BGB) scheitert.[83] Denn die Aktualisierungspflicht ist keine höchstpersönliche Pflicht.[84] Es steht dem Unternehmer frei, Dritte mit der Bereitstellung von Sicherheitsaktualisierungen zu beauftragen. Ein solcher Dritter ist insbesondere der Hersteller der Software bzw. der betroffenen Softwarekomponente, an den sich der Unternehmer wenden kann. Bei dieser Betrachtungsweise ist die Nacherfüllung durch die Einschaltung des Dritten grundsätzlich möglich, sofern der (Komponenten-)Hersteller bekannt und grundsätzlich bereit und in der Lage ist, die geschuldeten Aktualisierungen bereitzustellen. Es ist dann Aufgabe des Unternehmers, auf den Hersteller einzuwirken, damit dieser die Aktualisierungen bereitstellt. Dies wird dem Unternehmer umso leichter fallen, je besser er für diesen Fall bereits vertraglich Vorsorge getroffen hat. Einen gesetzlichen Anspruch auf Beseitigung nachträglicher Sicherheitsmängel im Wege der Nacherfüllung gewährt ihm jedenfalls der Regress nach §§ 327u I 2, 445a I BGB nicht, sondern nur einen entsprechenden Aufwendungsersatzanspruch. Ein eigener Anspruch auf Nacherfüllung gegenüber seinem Lieferanten kommt nur bei anfänglichen Sicherheitsmängeln in Betracht, sofern dieser im B2B-Verhältnis überhaupt besteht (dazu noch ausführlich unter C.I.).

Die Grenze für den Aufwand, den der Unternehmer betreiben muss, um den Hersteller zur Bereitstellung von Aktualisierungen zu bewegen, bildet dann das Kriterium

---

[83] In diese Richtung aber *Wendehorst*, in: Stabentheiner/Wendehorst/Zöchling-Jud (Hrsg.), Das neue europäische Gewährleistungsrecht, 111 (132), wonach der Regelfall ausbleibender Aktualisierungen Minderung und Vertragsbeendigung seien.

[84] Das verdeutlicht die Formulierung, der Unternehmer müsse die Bereitstellung von Updates „sicherstellen", Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 17.03.2021, 58 (BT-Drucksache 19/27653).

der „unverhältnismäßigen Kosten“ (§§ 327l II 1 Alt. 2, 275 II BGB). Weil der Unternehmer die Kosten der Nacherfüllung aufgrund der Regressregelungen in den §§ 327u I 2 bzw. 445a I, 478 BGB auf seinen Vertriebspartner umlegen und dieser sie über die gesamte Lieferkette bis zum Hersteller weiterreichen kann, ist im Rahmen der Unverhältnismäßigkeit der Kosten für die Bereitstellung der Sicherheitsaktualisierung nicht auf den Aufwand des Unternehmers abzustellen, sondern auf den Aufwand, der beim Hersteller für die Bereitstellung der Aktualisierung anfällt. Maßstab für die Unverhältnismäßigkeit ist daher auch nicht der Nutzen, den die Aktualisierung für den einzelnen Verbraucher hätte, der den Nacherfüllungsanspruch geltend macht, sondern der Nutzen für alle anspruchsberechtigten Anwender der Software.[85] Die Entwicklungskosten sind mit anderen Worten auf alle betroffenen Installationen, für die eine Aktualisierung geschuldet ist, zu verteilen und sodann zu ermitteln, ob die Kosten im Hinblick auf den dort erzielten Sicherheitsgewinn unverhältnismäßig hoch sind.

Eine faktische Beschränkung der Effektivität des Nacherfüllungsanspruchs ist allerdings, dass es äußerst unwahrscheinlich ist, dass einzelne Verbraucher ihre Vertragspartner auf die Bereitstellung von Sicherheitsaktualisierungen in Anspruch nehmen. Das beruht zum einen auf der Unkenntnis bzw. dem mangelnden Bewusstsein vieler Verbraucher hinsichtlich der Sicherheitsrisiken der Software. Zum anderen besteht ein allgemeines „rationales Desinteresse“ vieler Verbraucher, derartige „Kleinforderungen“ gerichtlich geltend zu machen. Und selbst wenn ein solcher Anspruch individuell erfolgreich eingeklagt werden sollte, bleibt die Frage der praktischen Vollstreckbarkeit eines entsprechenden Urteils auf Bereitstellung einer Sicherheitsaktualisierung gegen den Unternehmer nach §§ 887, 888 ZPO.

Im Hinblick auf diese gravierenden Einschränkungen des individuellen Rechtsschutzes dürfte den Instrumenten des kollektiven Rechtsschutzes, insbesondere der Abhilfeklage, wesentlich größere Bedeutung zukommen.[86]

2. Vertragsbeendigung und Minderung

Jenseits des Anspruchs auf Nacherfüllung stehen dem Verbraucher als Sekundärrechte das Recht zur Vertragsbeendigung bzw. zum Rücktritt (§§ 327i Nr. 2, 327m bzw. 437 Nr. 2, 323, 326 BGB) und das Minderungsrecht (§§ 327i Nr. 2, 327n bzw. 437 Nr. 2, 441 BGB) zu. Voraussetzung für die Geltendmachung dieser Rechte ist grundsätzlich, dass der Verbraucher zunächst erfolglos die Beseitigung des Sicherheitsmangels verlangt hat (§§ 327m I Nr. 2, 475d I Nr. 1 BGB), ein Nacherfüllungsversuch

[85] *Gsell*, in: Bach/Baldus/Beckmann u.a. (Hrsg.), Eckpfeiler des Zivilrechts, 8. Aufl. 2022, K. Rn. 76e; *Martens*, Schuldrechtsdigitalisierung, Rn. 296; so bereits der Umsetzungsgesetzgeber: BT-Drucksache 19/27653, 67.

[86] S. dazu den Beitrag von *Voß*, Kapitel 2 in diesem Band; ferner *Metzger*, FS Singer, 2021, 431 (438 ff.).

fehlgeschlagen ist (§§ 327m I Nr. 3, 475d Nr. 2 BGB[87]) oder dass es sich um einen schwerwiegenden Sicherheitsmangel handelt (§§ 327m I Nr. 4, 475d I Nr. 3 BGB).

Bei genauer Betrachtung zeigt sich allerdings, dass die besondere dogmatische Natur der Aktualisierungspflicht bei der Bestimmung der Rechtsfolgen von Vertragsbeendigung und Minderung nicht hinreichend berücksichtigt wurde. Besonders deutlich ist das bei den Vorschriften über Verträge über digitale Produkte, die hier nicht vollständig parallel zum Kaufrecht ausgestaltet sind.

So sieht beim Mietmodell § 327o III BGB vor, dass im Fall der Vertragsbeendigung der Anspruch des Unternehmers auch für bereits erbrachte Leistungen für denjenigen Teil des Bereitstellungszeitraums erlischt, in dem das digitale Produkt mangelhaft war. Diese Rechtsfolge erscheint dann unangemessen, wenn das Fehlen der Sicherheitsaktualisierung bzw. die vorhandene Sicherheitslücke sich auf die Nutzbarkeit des Produkts für den Verbraucher nicht ausgewirkt hat, etwa weil sie in dieser Zeit noch von keinem Angreifer ausgenutzt wurde. Hier sollte § 327o III 1 BGB dahingehend teleologisch reduziert werden, dass der Anspruch des Unternehmers erst ab dem Zeitpunkt erlischt, zu welchem der Mangel die Benutzung des Produkts durch den Verbraucher tatsächlich beeinträchtigte.[88]

Beim Kaufmodell sieht § 327o II BGB eigentlich die volle Rückerstattung des Preises vor, ohne dass der Verbraucher für die Zeit, in der er das Produkt uneingeschränkt verwenden konnte, Nutzungsersatz schuldet. Ebenso wie im Mietmodell erscheint das dann unangemessen, wenn die Nutzungsmöglichkeit durch das Bestehen einer Sicherheitslücke nicht eingeschränkt wurde. Das gilt erst recht, wenn eine bestimmte Softwareeigenschaft bei Bereitstellung noch gar keine Sicherheitslücke darstellte, sondern erst durch fortentwickelte Angriffsmethoden zu einer solchen wurde, was wiederum die Aktualisierungspflicht auslöste. Im Hinblick darauf, dass die Aktualisierungspflicht eine Dauerschuldkomponente begründet, die dem Mietmodell näher steht als dem klassischen Kaufvertrag, sollte hier die Regelung zum Mietmodell (§ 327o III BGB) analog angewendet werden,[89] sodass auch hier der Preis nur ab dem Zeitpunkt zu erstatten ist, zu welchem der Sicherheitsmangel die Nutzung des digitalen Produkts tatsächlich beeinträchtigte.

Beim Kauf von Waren mit digitalen Elementen tritt an die Stelle des Rechts zur Vertragsbeendigung das allgemeine Rücktrittsrecht (§§ 437 Nr. 2, 323 I BGB), wobei der

---

[87] Im Hinblick auf die Dauerschuldkomponente der Aktualisierungspflicht sollte diese Variante restriktiv ausgelegt werden, sodass eine sofortige Vertragsbeendigung wegen eines neuerlichen Mangels ausscheidet, wenn der Verbraucher das Produkt nach der Behebung einer Sicherheitslücke eine gewisse Dauer störungsfrei nutzen konnte, vgl. MüKoBGB/*Metzger*, § 327m Rn. 5; Schulze/Staudenmayer/*Gsell*, EU Digital Law, Art. 14 DCD Rn. 54; a.A. Erman BGB/*Bernzen/Specht-Riemenschneider*, § 327m Rn. 11.

[88] Ähnlich *Rieländer*, GPR 2022, 28 (34); Schulze/Staudenmayer/*Twigg-Flesner*, EU Digital Law, Art. 16 DCD Rn. 17 f.; Staudinger BGB/*Steinrötter*, § 327o Rn. 15 bezüglich Kompatibilitätseinschränkungen.

[89] *Gansmeier/Kochendörfer*, JURA 2022, 1447 (1453); Staudinger BGB/*Steinrötter*, § 327o Rn. 16; a.A. *Rieländer*, GPR 2022, 28 (34).

Verbraucher nach § 346 I, II 1 Nr. 1 BGB Wertersatz für die tatsächlich gezogenen Nutzungen schuldet.[90] Dieses Ergebnis scheint für den Rücktritt wegen ausgebliebener Sicherheitsaktualisierungen wesentlich angemessener als die Regelung in § 327o BGB.

Anstatt der Vertragsbeendigung kann der Verbraucher auch die Minderung seiner Gegenleistung wählen, also das digitale Produkt bzw. die Ware behalten, das Qualitätsdefizit akzeptieren und die Gegenleistung reduzieren (§§ 327n, 441 BGB). Denkbar ist, dass das Produkt an sich funktioniert, allerdings wegen Sicherheitsrisiken oder gar bereits eingetretener Sicherheitsvorfälle nur noch eingeschränkt nutzbar ist. Allerdings fällt es schwer, die allgemeine Minderungsformel – Reduktion des Preises proportional zur Wertminderung des Produkts – auf ausgebliebene Sicherheitsaktualisierungen anzuwenden, weil diese nicht per se zu einer entsprechenden Wertminderung führen. Hier muss schätzweise (§§ 327m III, 441 III 2 BGB) auf die mit der Sicherheitslücke einhergehenden Funktionseinschränkung abgestellt werden, die bei gravierenden Sicherheitslücken schnell 100 % betragen kann.

Außerdem sollte rechtsfolgenseitig § 327n II 2 BGB analog angewendet werden, sodass sich der Unternehmer auch nach Minderungserklärung noch eine entsprechende Aktualisierung bereitstellen und sich dadurch einen Teil der Gegenleistung verdienen kann.[91] Denn praktisch ist eine endgültige Minderung während des Aktualisierungszeitraums kaum umsetzbar, soweit die Minderung nach allgemeinen Grundsätzen darauf aufbaut, dass der Verbraucher im Gegenzug den Mangel hinnimmt, also auf die Sicherheitsaktualisierung verzichtet. Spätestens mit der nächsten Aktualisierung, die auf der vorherigen aufbaut, wird der Verbraucher auch von der zwischenzeitlich eingetretenen Schließung der Sicherheitslücke profitieren. Wendet man aus diesem Grund § 327n II 2 BGB analog an, wirkt die Minderung (auch) bei der punktuellen Bereitstellung nur für die vergangene Zeit der Funktionseinschränkung und der Unternehmer behält für die Zukunft sein Erfüllungsrecht und damit die Möglichkeit, sich für die Zukunft seine Gegenleistung zu verdienen.

All diese Konstellationen zeigen, dass die Dauerschuldkomponente der Aktualisierungspflicht bei der Bestimmung der Rechtsfolgen allenfalls unzureichend berücksichtigt wurde.[92]

---

[90] Umfänglich zu Rücktritt und Wertersatz bei Waren mit digitalen Elementen: *Schmidt-Kessel*, in: Schmidt-Kessel/Kramme (Hrsg.), Handbuch Verbraucherrecht, Kap. 13 Rn. 446 ff.

[91] Zu digitalen Produkten: Erman BGB/*Bernzen/Specht-Riemenschneider*, § 327n Rn. 11; *Gansmeier/Kochendörfer*, JURA 2022, 1447 (1455); zu Waren mit digitalen Elementen: BeckOK BGB/*Faust*, § 441 Rn. 14a; *Manhardt*, Die Aktualisierungspflicht beim Kauf von Waren mit digitalen Elementen, 2023, 185 ff.

[92] Dazu schon *Riehm/Abold*, CR 2021, 530 (538 f.); *Stierle*, IPRB 2021, 66 (69 f.); *Schmidt-Kessel*, in: Schmidt-Kessel/Kramme (Hrsg.), Handbuch Verbraucherrecht, Kap. 13 Rn. 317: „spürbares Spannungsverhältnis"; *Rieländer*, GPR 2021, 257 (267): „defizitär-lückenhafte Ausgestaltung".

3. Schadensersatz

Die praktisch wohl bedeutsamste Rechtsfolge ausgebliebener Sicherheitsaktualisierungen dürfte demnach der Schadensersatzanspruch des Verbrauchers sein. Dieser folgt beim Kauf von Waren mit digitalen Elementen aus §§ 437 Nr. 3, 280 ff. BGB, bei Verträgen über digitale Produkte aus §§ 327i Nr. 3, 280 ff.; 327m III 1 BGB. Besonders relevant ist hier zunächst der Anspruch auf Schadensersatz neben der Leistung, wenn der Verbraucher infolge einer Sicherheitslücke, die durch Angreifer ausgenutzt wurde, einen Schaden erlitten hat. Dieser ist als Mangelfolgeschaden grundsätzlich unter den Voraussetzungen des § 280 I BGB ersatzfähig.[93] Dabei ist zu beachten, dass – außer in Konstellationen des Vertrags mit Schutzwirkung zugunsten Dritter – der Anspruch nur dem Nutzer als Vertragspartner des Unternehmers zustehen kann, nicht Dritten, die aufgrund der Sicherheitslücke einen Schaden erlitten haben (etwa wegen einer DDoS-Attacke).

Die Pflichtverletzung im Sinne von § 280 I BGB liegt zunächst bei anfänglichen Sicherheitsmängeln in der Bereitstellung des Produkts mit einer Sicherheitslücke. Sofern diese Lücke allerdings für den Unternehmer bei Anwendung der im Verkehr erforderlichen Sorgfalt nicht erkennbar war, hat er diese Pflichtverletzung nicht zu vertreten. Bei dem Maß der geschuldeten Sorgfalt muss jedoch zwischen Herstellern und anderen Softwareverkäufern unterschieden werden. Während sich reine Verkäufer regelmäßig mit dem Nachweis exkulpieren können, die konkret in der Software vorhandene Schwachstelle sei nicht bekannt gewesen, muss ein Hersteller zudem nachweisen, er habe sie auch durch Softwareentwicklung nach dem Stand der Technik nicht vermeiden können. Sodann besteht aber die Möglichkeit, an die ausbleibende Bereitstellung von Sicherheitsaktualisierungen (als Nicht-Nacherfüllung) anzuknüpfen.[94] Insoweit ist der Maßstab des Vertretenmüssens schärfer: Auch wenn, wie oben (B.III.1.) dargelegt, der Unternehmer die Aktualisierung häufig nur mithilfe des (Komponenten-)Herstellers bereitstellen können wird, entspricht es der im Verkehr erforderlichen Sorgfalt, dass ein Anbieter digitaler Produkte sich vertraglich absichert, dass er zukünftige Sicherheitsaktualisierungen wird liefern können. Hat er dies unterlassen und verweigert dann der Hersteller die Bereitstellung einer erforderlichen Sicherheitsaktualisierung, so hat der Unternehmer das Ausbleiben der Aktualisierung zu vertreten.[95] Schließlich kommt

[93] Sofern nicht die Gewährleistung der IT-Sicherheit primärer Gegenstand der vertraglichen Leistungspflicht ist; anderenfalls, etwa beim Kauf eines Virenscanners, kann das Erfüllungsinteresse betroffen sein BeckOGK BGB/*Riehm*, 01.08.2023, § 280 Rn. 224.1.

[94] Zu der Debatte um die Einordnung der Nicht-Nacherfüllung als eigene Pflichtverletzung (Lehre von der doppelten Pflichtverletzung) oder als Perpetuierung der anfänglichen Pflichtverletzung (Lehre von der einheitlichen Pflichtverletzung) s. BeckOGK BGB/*Riehm*, § 280 Rn. 121 ff.

[95] Zur Notwendigkeit vertraglicher Abreden entlang der Lieferkette Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 119; *Janssen*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Smart Products, 91 (98); *Schmidt-Kessel*, ZfPC 2022, 117 (120) verweist in dem Zusammenhang auf die strukturelle Ähnlichkeit zur Kategorie des Übernahmeverschuldens.

als Pflichtverletzung auch die Verletzung der Aktualisierungspflicht aus §§ 327f I, 475b IV Nr. 2 BGB in Betracht.

Inhalt eines Anspruchs auf Ersatz der Mangelfolgeschäden kann insbesondere die Behebung von Schäden am eigenen IT-System sein, die infolge eines Angriffs eingetreten sind, bei dem die pflichtwidrig vorhandene Sicherheitslücke ausgenutzt wurde. Das kann etwa – in den Grenzen des § 251 II BGB – ein Anspruch auf Ersatz von Kosten für die Wiederherstellung des Systems sein,[96] aber auch auf Erstattung etwaiger „Lösegeldzahlungen" an Ransomware-Erpresser, die Daten verschlüsselt haben. Unter den Voraussetzungen der § 327m III bzw. §§ 437 Nr. 3, 280 I, III, 281, 283 BGB ist auch ein Anspruch auf Schadensersatz statt der Leistung denkbar, der z.B. auf den mangelbedingten Minderwert gerichtet sein kann, aber auch auf den Ersatz von Kosten für einen Workaround, durch den die Software trotz der Sicherheitslücke für den Verbraucher wieder nutzbar wird. Denkbar ist zudem ein Ersatz der Kosten für den Wechsel auf ein Alternativprodukt inklusive Migrationskosten. Ein Anspruch auf Ersatz der Kosten der Eigenentwicklung einer Sicherheitsaktualisierung bzw. ihrer individuellen Anfertigung durch einen Dienstleister wird allerdings in der Regel an § 251 II 1 BGB scheitern. Denn anders als im Rahmen der Nacherfüllung durch den Unternehmer, wo hohe Entwicklungskosten nicht zwingend die Unverhältnismäßigkeit (§§ 327l II 1 Fall 2, 439 IV 1 Fall 2 BGB) zur Folge haben,[97] profitiert bei der Anfertigung des Updates durch den Verbraucher (bzw. durch einen von diesem beauftragten Dienstleister) nur dieser selbst von der entwickelten Aktualisierung – nicht auch die übrigen Anwender.

C. Folgerungen für vertragliche Ansprüche im B2B-Verhältnis

Die vorstehenden Ausführungen beziehen sich ausschließlich auf das B2C-Verhältnis und sind nicht unmittelbar auf das B2B-Verhältnis übertragbar (§§ 327 I 1, 474 II 1 BGB). Insbesondere kommt eine pauschale analoge Anwendung der §§ 327 ff., 475b ff. BGB auf B2B-Verträge nicht in Betracht, weil ein Großteil dieser Regelungen spezifisches Verbraucherschutzrecht enthält.[98] Etwas anderes gilt nur partiell, wenn der B2B-Vertrag Teil einer Lieferkette ist, an deren Ende ein Verbraucher steht. In diesem Fall gelten besondere Regressvorschriften (§ 327u bzw. §§ 445a, 478 BGB), die dem Unternehmer entlang der Lieferkette einen Anspruch auf Ersatz der Nacherfüllungsaufwendungen gewähren, die er gegenüber dem Verbraucher zu tragen hatte

[96] BGH NJW 2009, 1066 (1067).

[97] Zur Notwendigkeit, die Nacherfüllungskosten (insbesondere die Entwicklungskosten) relativ nach der Zahl der profitierenden Gläubiger zu berechnen bereits oben unter B.III.1.

[98] MüKoBGB/*Metzger*, Vor § 327 Rn. 39; Staudinger BGB/*Steinrötter*, § 327 BGB Rn. 20.

(§§ 327u I 2, 445a I BGB). Im „reinen" B2B-Bereich außerhalb einer verbraucherbezogenen Lieferkette gilt jedoch lediglich das allgemeine Softwarevertragsrecht.

I. Anfängliche Sicherheitsanforderungen im B2B-Verkehr

Aber auch im allgemeinen Softwarevertragsrecht können Ansprüche auf Sicherheitsaktualisierungen bestehen. Wurde die Software aufgrund eines Werkvertrags hergestellt (Individualsoftware), so kann sich ein Anspruch auf Sicherheitsaktualisierungen als Nacherfüllungsanspruch ergeben, soweit die Sicherheit Bestandteil der Sollbeschaffenheit ist und das Werk bei Abnahme mangelhaft war. Gleiches gilt beim Kauf von Standardsoftware, wenn diese bei Gefahrübergang mangelhaft war. Der Dreh- und Angelpunkt bei diesen Vertragstypen liegt also in der Frage, ob eine später entdeckte oder aufgetretene Sicherheitslücke einen Sachmangel *bei Abnahme* bzw. *bei Gefahrübergang* darstellte.[99] Bei der Softwaremiete besteht nach §§ 535 I 2, 548a BGB[100] dagegen während der gesamten Vertragslaufzeit ein Anspruch des Mieters gegen den Vermieter auf Erhaltung der Software in einem zum vertragsgemäßen Gebrauch geeigneten Zustand. Dies verpflichtet jedenfalls dazu, dass anfängliche Abweichungen der geschuldeten Sollbeschaffenheit beseitigt werden.

Die unter B.I.2.a) vertretene Auslegung des Mangelbegriffs im Hinblick auf die Anforderungen an die Sicherheit folgt keinen verbraucherschutzrechtlichen Besonderheiten. Im Kaufrecht ergibt sich dies bereits daraus, dass ausschließlich die allgemeine Vorschrift des § 434 BGB zur Anwendung gelangt, die auch für B2B-Kaufverträge gilt. Aber auch bei B2B-Verträgen über die Bereitstellung digitaler Produkte können die vorstehend entwickelten Maßstäbe für die Sollbeschaffenheit auf den jeweils abhängig vom Vertragstyp[101] geltenden Mangelbegriff übertragen werden. Die Software entspricht somit auch im Rahmen des B2B-Verkehrs grundsätzlich nicht der vertraglichen Sollbeschaffenheit, wenn sie Sicherheitslücken enthält. Anders als im B2C können jedoch niedrigere Sicherheitsanforderungen vertraglich vereinbart werden, ohne dass die Anforderungen aus §§ 327h, 476 I 2 BGB beachtet werden müssen.

Im Gegensatz zum B2C-Verkehr besteht bei B2B-Kauf- oder Werkverträgen mangels gesetzlich geregelter Aktualisierungspflicht des Anbieters zudem keine Basis dafür, die Sollbeschaffenheit nicht nur auf den Zeitpunkt des Gefahrübergangs zu beziehen,

---

[99] Näher *Riehm*, in Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 201 (213 f.).

[100] Die h.M. ordnet auch die zeitweise Bereitstellung von Cloud-Diensten dem Mietrecht zu, BGH NJW 2007 (2394 f.); *Meents*, in: Borges/Meents (Hrsg.), Cloud Computing, 2016, § 4 Rn. 45 f.; *Duden*, Digitale Sachherrschaft, 2023, 283 f.; kritisch dazu *Riehm*, RDi 2022, 209 (211 ff.); im Einzelnen noch C.II.1.

[101] Zur vertragstypologischen Einordnung der Verträge über digitale Produkte *Gansmeier/Kochendörfer*, ZfPW 2022, 1 (24 ff.); zu Verträgen über digitale Dienstleistungen *Riehm*, RDi 2022, 209 ff.

sondern auf *evolvierende* Sicherheitsanforderungen (dazu oben B.I.2.c)). Ein Sicherheitsmangel, der im Wege der Nacherfüllung zu remedieren ist, besteht nur, wenn die Software bei Gefahrübergang bzw. bei Abnahme Eigenschaften aufweist, die zu diesem Zeitpunkt als potenzielles Einfallstor für Dritte angesehen werden können.

II. Vertragliche Aktualisierungspflichten im B2B-Verkehr

1. Vertragliche Aktualisierungspflichten im B2B-Mietmodell

Anders stellt sich die Situation bei Verträgen nach dem Mietmodell dar. Dort ist der Anbieter gem. §§ 535 I 2 Alt. 2, 548a BGB dazu verpflichtet, die Mietsache in einem Zustand zu erhalten, der einen vertragsgemäßen Gebrauch erlaubt. Unklar und umstritten ist allerdings, inwiefern dabei weiterentwickelte Sicherheitsanforderungen zu berücksichtigen sind.

Auf den ersten Blick scheint die Rechtsprechung zur Reichweite der mietrechtlichen Erhaltungspflicht (§ 535 I 2 BGB) dafür zu sprechen, dass Anpassungen an neue, weiterentwickelte Sicherheitsanforderungen nicht geschuldet sind. Danach richtet sich die über die Vertragslaufzeit geschuldete Beschaffenheit der (analogen) Mietsache grundsätzlich nach den Umständen des Vertragsschlusses – zu erhalten sind die Qualitätsstandards, die zu diesem Zeitpunkt oder zum Zeitpunkt des Baus der vermieteten Immobilie erwartbar waren.[102] Dies hindert die Vertragsparteien jedoch selbstverständlich nicht, eine dynamische Sollbeschaffenheit zu vereinbaren, die fortwährend zur Einhaltung des jeweiligen Stands der Technik verpflichtet.[103] Entscheidend ist vorliegend allein, *ob* eine solch dynamische Sollbeschaffenheit vertraglich vereinbart wurde, was ggf. im Wege der Auslegung zu ermitteln ist. Fehlt eine explizite Vereinbarung, ist dabei zwar grundsätzlich Vorsicht geboten, um das Äquivalenzverhältnis nicht zu stören.[104] Hinsichtlich veränderter Standards zur Vermeidung von Gesundheitsgefahren wird in Literatur und Rechtsprechung aber eine dynamische Sollbeschaffenheit auch ohne explizite Vereinbarung durchaus bejaht.[105] Denn ein Mieter erwartet berechtigterweise, dass die Mietsache seine Gesundheit während der gesamten Vertragsdauer nicht gefährdet.

---

[102] St. Rspr. seit BGH NJW 2004, 3174 (3175); MüKoBGB/*Häublein*, 9. Aufl. 2023, § 535 Rn. 120; *H. Hübner*, in: Lindner-Figura/Oprée/Stellmann (Hrsg.), Handbuch Geschäftsraummiete, 5. Aufl. 2023, 246; BeckOGK/*Schmidt*, 01.01.2024, § 535 BGB Rn. 316 f.

[103] *Gsell*, WuM 2022, 249 (250).

[104] Schmidt-Futterer/Börstinghaus BGB/*Lehmann-Richter*, 16. Aufl. 2024, § 535 Rn. 404; *Gsell*, WuM 2022, 249 (253).

[105] BayObLG NJW-RR 1999, 1533 (1535); MüKoBGB/*Häublein*, § 535 Rn. 123; *H. Hübner*, in: Lindner-Figura/Oprée/Stellmann (Hrsg.), Handbuch Geschäftsraummiete, 5. Aufl. 2023, Rn. 247.

Eine dynamische Sollbeschaffenheit hinsichtlich der Informationssicherheit entspricht auch den typischen Parteiinteressen bei Software-Mietmodellen. Dort ist das Interesse des Nutzers offenkundig darauf gerichtet, die Software während der gesamten Vertragsdauer sicher nutzen zu können. Es verwundert daher nicht, dass eine gewisse Dynamisierung der Sollbeschaffenheit von der untergerichtlichen Rechtsprechung und Literatur angenommen wird, indem Softwareanpassungen wegen nachträglicher gesetzlicher Änderungen als von der Erhaltungspflicht umfasst erachtet werden.[106] Gleichzeitig ist das Feld der Informationssicherheit hoch dynamisch, sodass eine anfänglich sichere Software binnen kürzester Zeit als unsicher gelten kann.[107] Für einen sicheren Gebrauch der Mietsache sind Sicherheitsaktualisierungen dann essenziell. Zudem muss der Vermieter die vermietete Software, wenn sie Gegenstand von Neuverträgen wird, ohnehin an veränderte Sicherheitsbedingungen anpassen werden, um den dann geltenden anfänglichen Qualitätsanforderungen zu entsprechen. Diese bereits angepasste Version kann ohne zusätzliche Kosten auch für Bestandskunden verfügbar gemacht werden. Angesichts dessen dürfte eine Auslegung von Software-Mietverträgen regelmäßig ergeben, dass die gemietete Software während der Vertragslaufzeit an *evolvierende* Sicherheitsanforderungen angepasst werden muss.[108]

Im B2B-Mietmodell ergibt sich somit für Sicherheitsanforderungen im Ausgangspunkt die gleiche Rechtslage wie im B2C-Verhältnis, weil der Vermieter nach §§ 535 I 2 Alt. 2, 548a BGB auch gegenüber unternehmerischen Mietern verpflichtet ist, während der gesamten Vertragslaufzeit die Sicherheit der vermieteten Software oder des vermieteten IoT-Geräts zu erhalten. Diese Erhaltungspflicht umfasst grundsätzlich auch eine Weiterentwicklung des Produkts, wenn sich die Sicherheitsanforderungen während der Vertragsdauer verändern. Faktisch wird die Pflicht zur Anpassung an veränderte Sicherheitsanforderungen oft jedoch daran scheitern, dass sich aus den vertraglichen Umständen etwas anderes ergibt. Wenn der Anbieter dem Nutzer etwa zeitgleich den Abschluss eines Softwarepflegevertrags anbietet, um die Software fortlaufend an aktuelle Sicherheitsanforderungen oder den Stand der Technik anzupassen, wird sich eine dynamische Sollbeschaffenheit nur schwer begründen lassen.

Die vorstehenden Erwägungen ergeben sich schließlich unabhängig von der vertragstypologischen Einordnung der Mietmodelle, die durchaus nicht alle dem Mietrecht unterliegen.[109] Denn auch bei einem Dauerwerkvertrag oder einem Dienstvertrag

---

[106] LG Wuppertal CR 2002 (7 f.); *Kremer*, ITRB 2013, 116 (117); *Raue*, CR 2018, 277 (278); *Marly*, Praxishandbuch Softwarerecht, Rn. 1346; *Redeker*, IT-Recht, Rn. 636.

[107] *Rockstroh/Kunkel,* MMR 2017, 77 (79).

[108] *Voigt*, IT-Sicherheitsrecht, Rn. 127; Schuster/Grützmacher/*Grützmacher*, IT-Recht, § 535 BGB Rn. 37; *Bartsch*, in: Verhandlungen des 71. Deutschen Juristentages, Band II/1, 2017, K11 (K24); a.A. *Roth-Neuschild*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 13 Rn. 73; *Meents*, in: Borges/Meents (Hrsg.), Cloud Computing, § 4 Rn. 77; *v. d. Bussche/Schelinski*, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, Teil 2.6 Rn. 158.

[109] S. zur vertragstypologischen Einordnungen der Verträge über digitale Dienstleistungen näher *Riehm*, RDi 2022, 209 ff.

sind die Anforderungen an die Qualität der Leistung – einschließlich der Sicherheit – zu bestimmen, und ob sich diese im Laufe der Vertragslaufzeit verändern. Das richtet sich vorrangig nach der vertraglichen Vereinbarung bzw. deren Auslegung, für die die gleichen Grundsätze gelten wie beim Mietvertrag.

2. Vertragliche Aktualisierungspflichten im B2B-Kaufmodell

Im B2B-Kaufmodell ergibt sich faktisch eine Aktualisierungspflicht aus dem allgemeinen Nacherfüllungsanspruch, soweit anfängliche Mängel betroffen sind (s.o. C.I.). Soweit allerdings eine Anpassung der Software an *evolvierende* Sicherheitsanforderungen in Rede steht, lässt sich eine Aktualisierungspflicht nach dem Vorbild der §§ 327f, 475b IV Nr. 2 BGB weder mit einer unmittelbaren noch mit einer analogen Anwendung dieser Vorschriften begründen. Vertreten wird zwar, dass diese Vorschriften zumindest im Regressverhältnis in einer Lieferkette, an deren Ende ein Verbraucher steht (§§ 327u, 445a, 478 BGB), analog anzuwenden seien.[110] Allerdings dürfte eine Analogie hier am Fehlen einer planwidrigen Regelungslücke scheitern,[111] denn §§ 327u I 2, 445a I BGB zeigen, dass der Gesetzgeber die Folgen der Aktualisierungspflicht im Regressverhältnis durchaus regeln wollte, sich aber dafür entschieden hat, insoweit lediglich einen Aufwendungsersatzanspruch und gerade keine eigene Aktualisierungspflicht des Vertriebspartners vorzusehen. Auf §§ 327e I 2, III 1 Nr. 5, 327f bzw. 475b II, IV Nr. 2 BGB, die einerseits die Aktualisierungspflicht im B2C begründen und andererseits die Folgen ihrer Verletzung dem Gewährleistungsrecht zuordnen, verweisen weder § 327u BGB noch §§ 445a, 478 BGB.

Ob die Lösung über einen Anspruch auf Aufwendungsersatz allerdings den zugrundeliegenden Richtlinien entspricht, ist zweifelhaft. Denn Art. 20 DIDRL und Art. 18 WKRL sehen vor, dass Unternehmer in der Lage sein sollen, vorherige Glieder der Vertriebskette in Regress zu nehmen, wenn die Vertragswidrigkeit durch ein „Handeln oder Unterlassen" vorheriger Kettenglieder verursacht wurde. Dass zu den regressfähigen Vertragswidrigkeiten auch die Fälle ausbleibender Aktualisierungen gehören sollen, zeigen Art. 18 S. 1 und Erwägungsgrund 63 S. 2 WKRL[112]. Damit soll sichergestellt werden, dass die mit (fehlenden) Aktualisierungen einhergehenden Kosten nicht endgültig vom Handel getragen werden müssen, sondern diese entlang der Kette weitergegeben werden können.[113] Dieses Ziel verfehlt jedoch die Umsetzung im BGB. Denn faktisch wird der Weg über den Aufwendungsersatzanspruch aus §§ 327u I 2,

[110] *Hoffmann/Löffler*, ZfPW 2023, 1 (16 f.).

[111] So auch *Sosnitza*, FS Becker-Eberhard, 535 (542 f.).

[112] Das Fehlen dieser Vorgabe i.R.d. DIDRL sollte nicht zu einem Umkehrschluss verleiten, *Martens*, Schuldrechtsdigitalisierung, Rn. 480.

[113] ErwG 78 S. 2 DIDRL, ErwG 63 S. 1 WKRL.

445a I BGB meist ausscheiden, da Nacherfüllungsaufwendungen in Bezug auf Aktualisierungen beim Handel kaum anfallen, sofern nicht ausnahmsweise der Quellcode der Software bekannt ist.[114] Einen Ersatz der Aufwendungen für Vertragsbeendigung und Minderung des Verbrauchers infolge ausbleibender Aktualisierungen sehen §§ 327u I 2, 445a I BGB jedoch nicht vor.[115] Nur bei anfänglichen Sicherheitsmängeln ist es dem Handel daher möglich, zumindest die Aufwendungen für die Nacherfüllung entlang der Lieferkette weiterzugeben oder selbst vom Vertrag zurückzutreten. Bei nachträglichen Veränderungen der Sicherheitsanforderungen trägt der Handel – entgegen dem Willen des Unionsgesetzgebers – dagegen letztlich doch die Kosten ausbleibender Aktualisierungen. Um das Problem zu umgehen, könnte den Regressvorschriften entnommen werden, dass sie hinsichtlich nachträglicher Veränderungen der Sicherheitsanforderungen pflichtenbegründend wirken und so entlang der Lieferkette einen unechten Regress ermöglichen.[116] Angesichts der eindeutigen gesetzgeberischen Entscheidung für einen reinen Aufwendungsersatzanspruch,[117] wird sich ein derartiges Ergebnis methodisch allerdings kaum noch im Rahmen der richtlinienkonformen Rechtsfortbildung erreichen lassen.[118] Hier muss der Gesetzgeber Abhilfe schaffen.

Teilweise wird sogar erwogen, dass Aktualisierungspflichten zukünftig auch beim „reinen" B2B-Softwarekauf als nachwirkende Nebenleistungspflicht konkludent vereinbart seien, wenn es an einer gegenteiligen Klausel fehlt.[119] Allerdings würde selbst diese Konstruktion nicht dazu führen, dass das Ausbleiben der Aktualisierungen als Sachmangel zu klassifizieren ist, gilt doch die Verschiebung des Bezugszeitpunkts aus

---

[114] *Lorenz*, NJW 2021, 2065 (2067 f.); BeckOK BGB/*Faust*, § 445a Rn. 18a; *Dubovitskaya*, MMR 2022, 3 (7).

[115] Anders dagegen in Fällen der unterbliebenen Bereitstellung, wo Aufwendungen für die Vertragsbeendigung gem. §§ 327u I 1, 327c I 1 BGB ersatzfähig sind. Das dürfte auch einer teleologischen Extension des § 327u I 2 BGB auf Ersatz der Kosten für Vertragsbeendigung und Minderung entgegenstehen; a.A. *Jung/Rolsing*, ZfDR 2024, 27 (51).

[116] *Schmidt-Kessel*, ZfPC 2022, 117 (124); nach *Pfeiffer*, GPR 2022, 223 (233) besteht zwar entlang der Lieferkette eine Aktualisierungspflicht, ihre Verletzung begründet aber keinen Sachmangel; a.A. BeckOK BGB/*Faust*, § 445a Rn. 18a, wonach sich die Pflichtenerweiterung auf den Aufwendungsersatzanspruch beschränkt; nach MüKoBGB/*Metzger*, § 327u Rn. 8; *Blanke-Roeser*, JZ 2024, 126 (129) setzt sogar der Aufwendungsersatz eine Aktualisierungsvereinbarung zwischen Unternehmer und Vertriebspartner voraus.

[117] Die Beschlussempfehlung des Rechtssauschusses des Bundestags verweist hinsichtlich der Frage, wie der Handel die Bereitstellung von Aktualisierungen sicherstellen könne, explizit darauf, er müsse sich selbst vertraglich ggü. seinen Vertriebspartnern absichern: Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss) vom 23.06.2021, 7 (BT-Drucksache 19/31116).

[118] Zum Willen des nationalen Umsetzungsgesetzgebers als Grenze richtlinienkonformer Rechtsfortbildung *Langenbucher/Donath*, in: Langenbucher (Hrsg.), Europäisches Privat- und Wirtschaftsrecht, 5. Aufl. 2022, § 1 Rn. 110 ff.

[119] *Hoffmann/Löffler*, ZfPW 2023, 1 (17 f.); schon zur alten Rechtslage diesbezüglich *Regenfus*, JZ 2018, 79 (82); *Raue*, CR 2018, 277 (278).

§ 475b II BGB allein im B2C-Verhältnis.[120] Zudem sind derartige Aktualisierungspflichten der typische Inhalt eines Softwarepflegevertrages, der in der Regel entgeltlich abgeschlossen wird. Die Annahme einer konkludenten Vereinbarung von *unentgeltlichen* Aktualisierungspflichten beim Kaufvertrag ist mit dem Leitbild des entgeltlichen Softwarepflegevertrags nicht vereinbar und kann den Parteien daher grundsätzlich nicht unterstellt werden.

Umso wichtiger ist es somit, im B2B-Verhältnis Aktualisierungspflichten ausdrücklich zu vereinbaren – unabhängig davon, ob es sich um ein Regressverhältnis im Sinne von §§ 327u, 478 I BGB handelt oder einen „reinen" B2B-Vertrag. Derartige Vereinbarungen sollten die Voraussetzungen der Aktualisierungspflicht und die Rechtsfolgen ihrer Verletzung detailliert regeln. Aufgrund des Leitbilds des Kaufvertrags als punktuellem Leistungsaustausch und des Regelfalls *entgeltlicher* Softwarepflegeverträge ist auch die Vorgabe unentgeltlicher Aktualisierungspflichten in AGB eines Abnehmers problematisch, weil eine solche Klausel typischerweise nach § 307 I, II Nr. 1 BGB unwirksam sein dürfte. Diese Beurteilung kann sich erst dann ändern, wenn die B2B-Vertragspraxis sich langfristig an die Verbraucherschutzvorschriften angleicht und damit das Leitbild des B2B-Softwarevertrags verändert.[121]

Problematisch bleibt stets die Abgrenzung zwischen Nacherfüllungsansprüchen, die auch im B2B-Verhältnis für anfängliche Mängel (soeben C.I.) bestehen, und weitergehenden Aktualisierungspflichten aus einem Softwarepflegevertrag. Letztere sind typischerweise auf die Weiterentwicklung der Software selbst (Upgrade) sowie auf die Anpassung an einen weiterentwickelten Stand der Technik oder neue Sicherheitsanforderungen gerichtet.[122] Hier droht die teilweise Unwirksamkeit der Vergütungsklauseln wegen Doppelvergütung, soweit eine Vergütung auch für die Beseitigung anfänglicher Mängel vorgesehen ist.[123]

III. Auswirkungen des künftigen Cyber-Resilience-Acts

Der zukünftige Cyber-Resilience-Act wird eine neue Verantwortung des Herstellers von Software für die Bereitstellung von Sicherheitsaktualisierungen während der gesamten Lebensdauer begründen (Art. 13 VIII UA 1 CRA). Sein Anwendungsbereich umfasst dabei auch Produkte, die allein für den Unternehmermarkt bestimmt sind. Wenn in Umsetzung einer solchen Regelung zukünftig Hersteller verpflichtet sind,

[120] *Wendehorst*, JZ 2021, 974 (980 f.); *Pfeiffer*, GPR 2022, 223 (233).

[121] Für die Berücksichtigung der §§ 327 ff. BGB im B2B MüKoBGB/*Metzger*, Vor § 327 Rn. 39 f.

[122] Im Einzelnen unterscheiden sich die Leistungsinhalte von Softwarepflegeverträgen erheblich: *Schneider/Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 14 Rn. 88 ff.

[123] Dazu *Marly*, Praxishandbuch Softwarerecht, Rn. 1050 ff.

während der gesamten Nutzungsdauer der Software kostenlos Sicherheitsaktualisierungen bereitzustellen, kann dies Auswirkungen auf das vorstehend beschriebene gesetzliche Leitbild haben. Es besteht dann auch bei Kauf- und Werkverträgen kein Grund mehr, Sicherheitsaktualisierungen, deren Erforderlichkeit sich aus einer Weiterentwicklung der Sicherheitsanforderungen ergibt, dem Leitbild des entgeltlichen Softwarepflegevertrags zuzuordnen. Vielmehr kann dann jedem Glied der Lieferkette zugemutet werden, derartige Sicherheitsaktualisierungen unentgeltlich weiterzureichen. Eine entsprechende Regelung in AGB der Abnehmer, die eine Verpflichtung des Lieferanten zur unentgeltlichen Bereitstellung von Sicherheitsaktualisierungen vorsieht, müsste dann als zulässig angesehen werden.

D. Ergebnis

Die vorstehenden Ausführungen haben gezeigt, dass das geltende Privatrecht, insbesondere das Produkthaftungsrecht und das Recht der Verträge über digitale Produkte sowie der Kaufverträge über Waren mit digitalen Elementen, einen erheblichen Beitrag zur „digitalen Resilienz“ leisten kann. Sofern die gesetzlich vorgesehenen Ansprüche auch tatsächlich durchgesetzt werden, sollte die Versorgung digitaler Systeme in Verbraucherhand mit Sicherheitsaktualisierungen gesichert sein. Im B2B-Verkehr ist hingegen mehr vertragliche Vorsorge und damit Eigeninitiative der Vertragsparteien gefragt. In jedem Fall hängt die tatsächliche Schaffung digitaler Resilienz durch Sicherheitsaktualisierungen aber von der praktischen Durchsetzung der bestehenden Rechte und Ansprüche ab. Im Hinblick auf Verbraucher könnte die Abhilfeklage nach dem VDuG hierfür ein wirksames Instrument sein.

Staatliche Verantwortung für sichere Software

Christian Ernst

Meldungen, die sich mit Hackerangriffen befassen, finden sich mittlerweile täglich in den Nachrichten. Betroffen sind davon Institutionen aus ganz unterschiedlichen Bereichen. Immer wieder richten sich solche Angriffe nicht nur gegen Akteure des rein privaten Wirtschaftslebens, sondern auch Institutionen mit besonderer Bedeutung für das Gemeinwesen, wie Klinikbetreiber oder Versorgungsunternehmen aus dem Bereich der Daseinsvorsorge.[1] Solche Fälle zeigen stets wieder, dass sich Software und IT-Systeme zu einer Achillesferse moderner Gesellschaften entwickelt haben. Der Frage, inwiefern eine staatliche Verantwortung für sichere Software besteht, soll diese Abhandlung nachgehen. Sie zielt darauf ab, die Strukturen einer staatlichen Verantwortung herauszuarbeiten und ihre Erscheinungsformen zu kategorisieren. In einem ersten Schritt sollen zu diesem Zweck Vorüberlegungen zu den Elementen der Sicherheit und der Schutzgüter angestellt werden. Im Anschluss sollen die rechtlichen Grundlagen einer staatlichen Verantwortung untersucht werden. Mit welchen unterschiedlichen Maßnahmen der Staat seiner Verantwortung für sichere Software nachkommt, wird in einem dritten Teil betrachtet.

A. Vorüberlegungen und Rahmenbedingungen

Die Frage nach einer staatlichen Verantwortung für sichere Software ist geprägt durch Elemente, die wesentlich von subjektiven Standpunkten abhängen und deshalb eine gewisse Unschärfe in sich tragen. Wann ist eine Software „sicher"? Das Gesetz hilft dabei nur wenig, weil Software an sich selten ein Anknüpfungspunkt für gesetzliche Regelungen ist. Und welchen Personen, Gütern und Interessen gegenüber oder für welche Anwendungsfelder von Software ist der Staat „verantwortlich"?

[1] Siehe etwa: Hackerangriff auf Uniklinik in Frankfurt, Frankfurter Allgemeine Zeitung v. 8.10.2023, https://www.faz.net/aktuell/rhein-main/frankfurt/uniklinik-frankfurt-erholung-nach-hacker-angriff-wird-wochen-dauern-19229859.html; *Dammann*, Cyber-Attacke auf den Trinkwasserverband Stade, Kreiszeitung Neue Buxtehuder Wochenblatt v. 4.8.2023, https://www.kreiszeitung-wochenblatt.de/horneburg/c-blaulicht/cyber-attacke-auf-den-trinkwasserverband-stade_a289431; vgl. allgemein: Hackerangriff legt IT-Infrastruktur von 70 Kommunen lahm, Zeit Online v. 31.10.2023, https://www.zeit.de/digital/2023-10/cybersicherheit-hackerangriff-cyberangriff-kommunen-nrw (letzter Zugriff jeweils: 04.04.2024) sowie den Nachw. in Fn. 9.

I. Sicherheit

In einem engen oder integritätsbezogenen Sinn liegt dem Verständnis von Sicherheit in erster Linie die von außen kommende Einwirkung auf Software zugrunde.[2] Gemeint ist damit vor allem die Einflussnahme oder Einwirkung Unbefugter auf Software. Dahinter stehen wiederum häufig Gefahren für Daten, die durch den Eingriff in die Software hervorgerufen werden und die in einer inhaltlichen Verfälschung, sachfremden Nutzung, unbefugten Weitergabe oder der fehlenden Verfügbarkeit von Daten resultieren können.[3] Hackerangriffe und der Einsatz verschiedenster Formen von Malware sind mittlerweile in allen Lebensbereichen an der Tagesordnung; dabei werden auch immer wieder Werkzeuge verwendet, die genauso von staatlicher Seite eingesetzt werden. Unbefugt in diesem Sinne können also vor allem Dritte sein – es ist aber auch nicht ausgeschlossen, dass von diesem Sicherheitsverständnis der Staat und seine Behörden selbst als Gefahrenquellen angesprochen sind.

Dieses Sicherheitsverständnis findet sich etwa im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), wenn dort z.B. in § 2 Abs. 2 auf den Schutz vor „Angriffen und unautorisierten Zugriffen" abgestellt wird. Auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – das im Folgenden als IT-Grundrecht bezeichnet wird – liegt ein derartiges Sicherheitsverständnis zugrunde, weil es an den Zugriff auf das System anknüpft, durch den Leistung, Funktion oder Speicherinhalte für Dritte zugänglich werden und so Ausspähung, Überwachung oder Manipulation ermöglicht werden.[4] Dieses vom Bundesverfassungsgericht vor 15 Jahren aus dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) neu abgeleitete Grundrecht macht dabei besonders deutlich, dass dieses integritätsbezogene Sicherheitsverständnis in einem engen Zusammenhang mit einer datenschutzzentrierten Struktur steht.[5]

Es soll hier nicht unberücksichtigt bleiben, dass Sicherheit auch in einem weiten, stärker funktional-normativen Sinn beschrieben werden kann. Sicherheit von Software kann nämlich auch dahingehend verstanden werden, dass Software, unabhängig vom Einwirken unbefugter Dritter, normative Vorgaben bei ihrem Einsatz einhält und keine ungewollten Ergebnisse produziert. Dies bezieht sich etwa auf automatisierte Entscheidungssysteme, die auf Grundlage rechtlich zulässiger Verwendungs- und Entscheidungskriterien zu rechtlich zulässigen Ergebnissen kommen. Bei dieser Perspektive

---

[2] Vgl. *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. EL Mai 2022, Ziff. 50.1 Rn. 6.

[3] BVerfGE 120, 274 (314); *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 6 m.w.N.; *Ernst*, Der Grundsatz digitaler Souveränität, 2020, 35 ff.

[4] BVerfGE 120, 274 (314).

[5] Vgl. *Britz*, DÖV 2008, 411 (411); *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. EL Mai 2022, Ziff. 50.1 Rn. 303.

wird die Sicherheit also nicht durch externe Einflüsse erschüttert, sondern die von vornherein in der Software selbst angelegte Funktionsweise. Für diese Art von Sicherheitsbedenken werden allerdings deutlich andere rechtliche Rahmenbedingungen diskutiert als die, die für das unbefugte Einwirken Dritter auf Software in Betracht kommen, etwa das Verhältnis von automatisierten zu menschlichen Entscheidungen oder Fragen der Gleichbehandlung.[6] Sie sollen deshalb hier nicht berücksichtigt werden.

Ebenfalls nicht berücksichtigt werden soll eine Verantwortung, die den Umgang mit Software und ihre Verwendung zum Gegenstand hat. Dem liegt die Unterscheidung zwischen technischen und organisatorischen Maßnahmen zugrunde, wie sie schon in der Datenschutzrichtlinie aus dem Jahr 1995 angelegt war und heute in vielen Normen zur IT-Sicherheit Niederschlag gefunden hat. Solche organisatorischen Maßnahmen können sich etwa auf Maßnahmen zum Betriebsablauf und Anweisungen an das Personal beziehen,[7] aber nicht auf unmittelbare Eigenschaften von Software.

II. Schutzgüter

Um sich einer staatlichen Verantwortung für sichere Software anzunähern, kann weiter eine schutzgutbezogene Betrachtung des Sicherheitsbegriffs helfen. Das BSIG nimmt für die geschützten Güter mehrfach auf das polizeirechtliche Element der öffentlichen Sicherheit Bezug.[8] Eine staatliche Verantwortung für sichere Software umfasst bei diesem Blickwinkel auch den Schutz subjektiver Rechte und Rechtsgüter des Einzelnen. Dabei kann die gesamte Bandbreite privater Tätigkeiten berührt sein, von rein privatnützigen Anwendungen bis zu gemeinwohlorientierten Betätigungen der Daseinsvorsorge in privater Hand. Software kann höchst unterschiedliche Bedeutungen aufweisen, so dass, abhängig von der Bewertung einer konkret betroffenen Software, unterschiedlichste staatliche Reaktionen erforderlich werden können.

Die Einrichtungen des Staates – ebenfalls ein klassisch polizeiliches Schutzgut – sind erheblich verletzlicher durch unsichere Software als durch herkömmliche Gefahren im analogen Geschehen. Große Aufmerksamkeit hat etwa der Hackerangriff auf den Deutschen Bundestag im Jahr 2015 erfahren. Aber auch wenn das Ziel weniger prominent ist, können erhebliche Auswirkungen drohen. Der Landkreis Anhalt-Bitterfeld wurde 2017 erpresst, nachdem ein Hackerangriff den Verwaltungsbetrieb lahmgelegt hatte. In Folge dessen war unter anderem eine Auszahlung von Sozial- und Unterhaltsleistungen für etwa eine Woche nicht möglich und eine Umweltdatenbank musste neu

[6] Dazu etwa *Martini*, JZ 2017, 1017; *Ernst*, JZ 2017, 1026; *Steege*, MMR 2019, 715; *Wischmeyer*, AöR 143 (2018), 1; *Hartmann*, EuZA 2019, 421.

[7] *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. EL Mai 2022, Ziff. 50.1 Rn. 284.

[8] Korrespondierend damit sind auch die Polizei- und Ordnungsbehörden im digitalen Raum prinzipiell für die Gefahrenabwehr zuständig, dazu *Gruber/Brodowski/Freiling*, GSZ 2022, 171.

aufgebaut werden.[9] Dieser erste „Cyber-Katastrophenfall" Deutschlands verdeutlicht, dass die Fähigkeit zur Wahrnehmung und Erfüllung staatlicher Aufgaben mittlerweile in einem erheblichen Maße vom ordnungsgemäßen Funktionieren eingesetzter Software und der Möglichkeit zum jederzeitigen Datenzugriff abhängt. Der Verlust der Funktionsfähigkeit der Software kann gleichbedeutend sein mit dem – meist vorübergehenden – Verlust einer staatlichen Fähigkeit an sich.

Im Sinne eines Schutzguts der objektiven Rechtsordnung fordert staatliche Verantwortung dann auch das Etablieren eines effektiven staatlichen Regelungsrahmens zur Aufrechterhaltung sicherer Software sowie das Einhalten dieser Regelungen.[10] Das bedeutet, dass die staatliche Gewalt, unabhängig von einer konkreten Gefährdung, effektive Regelungen zur Sicherstellung sicherer Software zu erlassen, über ihre Einhaltung zu wachen und diesen notfalls zur Durchsetzung zu verhelfen hat.

B. Rechtliche Grundlagen einer staatlichen Verantwortung

I. Verantwortung als rechtliches Element

Mit diesen Überlegungen im Hintergrund sollen die rechtlichen Grundlagen einer staatlichen Verantwortung betrachtet werden. Verantwortung kann in einem ersten Schritt ein positiver oder negativer Kontext verliehen werden.[11] In einem negativen Zusammenhang hat das Verantwortungssubjekt für ein bestimmtes, vom Sollzustand negativ abweichendes Ergebnis einzustehen. Diese Form der ex-post Verantwortung kann zum Beispiel zu Schadensersatzverpflichtungen, individueller Strafbarkeit oder im politischen Kontext zu Rücktritten führen, sofern das Verantwortungssubjekt kausal verantwortlich für die eingetretene Abweichung ist. Zielt die Verantwortung hingegen auf einen positiv umschriebenen Zustand ab, hat das Verantwortungssubjekt auf diesen Zustand, soweit er noch nicht vollständig erreicht ist, hinzuwirken oder hat ihn zu bewahren.

Für die Sicherheit von Software geht es, das macht das integritätsbezogene Sicherheitsverständnis deutlich, um die Abwesenheit von Einwirkungen Unbefugter. Das ist als solches ein positiver Zustand, ein Optimum. Das bedeutet nicht, dass es auf diesem Feld nicht auch nachträgliche Maßnahmen aufgrund einer staatlichen Verantwortung geben könnte. Die Verantwortung des Staates für sichere Software zielt aber wie bei der allgemeinen polizeirechtlichen Gefahrenabwehr in erster Linie auf das Erreichen und

[9] *Laaff*, Wie eine Cyberattacke einen ganzen Landkreis lahmlegt, Zeit Online v. 12.7.2021, https://www.zeit.de/digital/datenschutz/2021-07/hackerangriff-anhalt-bitterfeld-cyber-katastrophenfall-kommunen-internetkriminalitaet (letzter Zugriff: 04.04.2024).

[10] *Wischmeyer*, in: Hill/Mehde (Hrsg.), Herausforderungen für das Verwaltungsrecht, 2023, 133 (146).

[11] Dazu und zum Folgenden: *Klement*, Verantwortung, 2006, 50 ff.

Bewahren eines sicheren Zustands und damit das Bestehen und die Reichweite einer ex-ante Verantwortung ab. In der Sache ist also eine potenzielle Wirkmacht zum Erreichen und Bewahren eines angestrebten Zustands angesprochen. Der öffentliche Diskurs kreist hier im Allgemeinen darum, wer die Verantwortung konkret trägt bzw. welchen Anteil ein bestimmtes Subjekt – hier der Staat – daran hat.

Über eine tatsächliche potenzielle Wirkmacht hinaus bedarf es zur Annahme einer Verantwortungsbeziehung zwischen dem Staat und der Softwaresicherheit einer Norm oder einem Komplex von Normen, die den Staat zu diesem Ziel bzw. zu dieser Aufgabe verpflichten. Denn nur weil der Staat etwas erreichen oder fördern *kann*, *muss* er dies noch längst nicht.[12] Damit ist die Frage nach der Quelle von Staatszwecken, Staatszielen und insbesondere von Staatsaufgaben aufgeworfen.

Einen bestimmten oder gar abschließenden Katalog an Staatsaufgaben enthält das Grundgesetz nicht. Der formelle Staatsaufgabenbegriff, der weite Akzeptanz erfahren hat, qualifiziert all solche Aufgaben als Staatsaufgaben, denen sich ein Träger von Staatsgewalt tatsächlich in legitimer Weise annimmt.[13] Das erfordert weder eine überstaatliche Verpflichtung noch eine ausdrückliche Ermächtigung.[14] Es ist schon ausreichend, dass der einfache Gesetzgeber die Sicherheit von Software durch Gesetz als Verwaltungsaufgabe bestimmt hat, wie es zum Beispiel durch § 3 Abs. 1 S. 1 BSIG geschehen ist. Solche Vorschriften beziehen sich allerdings regelmäßig nur auf einen Ausschnitt des zugrunde liegenden Aufgabenfeldes und wenden sich auch nicht an den Staat als Ganzes unter Berücksichtigung des Normgebers. Verpflichtungen auf der Ebene des Verfassungsrechts lassen sich aus solchen einfachgesetzlichen Regelungen jedenfalls nicht herleiten.

II. Grundrechte als Ursprung einer staatlichen Verantwortung für sichere Software

Grundrechte wirken klassischerweise als Abwehrrechte und können als solche gegen Grundrechtseingriffe schützen, die sich in einer aktiven Verschlechterung der Softwaresicherheit oder Ausnutzung unsicherer Software durch den Staat selbst manifestieren.[15] Hierdurch können etwa das Fernmeldegeheimnis aus Art. 10 GG, das Recht auf informationelle Selbstbestimmung und das IT-Grundrecht verletzt werden. Das

[12] Vgl. *Klement*, Verantwortung, 2006, 88.

[13] „Aktuelle Staatsaufgaben" in der Terminologie von *Isensee*, in: HStR IV, 3. Aufl. 2006, § 73 Rn. 13; BVerfGE 12, 205 (243); *Burgi*, Privatisierung öffentlicher Aufgaben – Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf, Gutachten für den 67. DJT, 14 f.

[14] Grundlegend zum Dogma der Allzuständigkeit: *Isensee*, in: HStR IV, 3. Aufl. 2006, § 73 Rn. 55 ff.

[15] Eingehend zur Rolle des Staats als Gefährder der Informationssicherheit und den grundrechtlichen Grenzen: *Wischmeyer*, Informationssicherheit, 2023, 129 ff., 279 ff. Abgrenzungsprobleme zur Schutzpflichtdimension bestehen hinsichtlich der Vorgaben für Beschaffenheit, Funktionalität und Anwendungskontrolle von Überwachungssoftware; dies wurde offen gelassen in BVerfG (K) NVwZ-RR 2022, 401 Rn. 19.

Bundesverfassungsgericht hat in seiner Entscheidung zu IT-Sicherheitslücken zu Recht anerkannt, dass die Freiheitsverwirklichung im Allgemeinen und die allgemeine Entfaltung der Persönlichkeit auf die Nutzung informationstechnischer Systeme angewiesen ist und dass in diesem Bereich ein Gefährdungspotenzial besteht, das weit über die Offenbarung persönlichkeitsrelevanter Informationen hinaus geht.[16] Es folgert daraus eine staatliche Verpflichtung zum Schutz vor Angriffen Dritter auf solche Kommunikation, die dem Art. 10 Abs. 1 GG unterfällt, und informationstechnische Systeme, wie sie vom IT-Grundrecht erfasst sind. Für eine solche staatliche Schutzpflicht spricht auch die erhebliche Macht privater Unternehmen im Bereich der Informationstechnologien. Regelmäßig finden Gefahren ihren Ursprung im privaten Bereich. Rechtlicher Ausgangspunkt ist für das Gericht eine objektive Werteentscheidung der Verfassung, die in den Grundrechten des Art. 10 Abs. 1 GG und des IT-Grundrechts enthalten ist. Dahinter steht die allgemeine staatliche Verantwortung zur Gewährleistung von Sicherheit.[17]

Dieser Gedanke einer staatlichen Verpflichtung zum Schutz kann erweitert werden auf solche Konstellationen, in denen andere als die beiden bislang genannten grundrechtlichen Gewährleistungen betroffen sind.[18] Das offensichtlichste Beispiel dafür findet sich im Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG). Ein Bezug zur Nutzung von Software und IT-Systemen kann sich im Hinblick auf die von Anlagen ausgehenden Umweltgefahren[19] oder die Gewährleistung einer Gesundheits-[20] und Energieinfrastruktur[21] ergeben.[22] Die Ausübung wirtschaftlicher Freiheiten und die Versorgung der Bevölkerung mit wichtigen Gütern setzen ebenfalls auf die Nutzung informationstechnischer Systeme, so dass die Berufsfreiheit (Art. 12 Abs. 1 GG) und die Eigentumsgarantie (Art. 14 GG) berührt werden. Im Falle der unbefugten

---

[16] BVerfGE 158, 170 Rn. 26 ff. – *IT-Sicherheitslücken* mit Zitat und Literaturnachweisen in Rn. 33 und 37. Zuletzt auch BVerfG (K) NVwZ-RR 2022, 401 Rn. 17. Zustimmend *Wischmeyer*, in: Hill/Mehde (Hrsg.), Herausforderungen für das Verwaltungsrecht, 2023, 133 (146); zuvor u.a. bereits *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005, 90 ff.; *Hoffmann-Riem*, JZ 2008, 1009 (1013 ff.); *Heckmann*, FS Käfer, 2009, 129; vorsichtig *Möllers/Pflug*, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, 47 (58 ff.).

[17] *Wischmeyer*, Informationssicherheit, 2023, 156 ff. m.w.N.

[18] *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. EL Mai 2022, Ziff. 50.1 Rn. 392.

[19] Grundlegend zu den Gefahren der Kernenergienutzung: BVerfGE 49, 89 (141 f.) – *Kalkar*; 53, 30 (57 ff.) – *Mülheim-Kärlich*.

[20] Zu deren Gewährleistung als Pflicht des Staates: BVerfGE 159, 223 Rn. 167 ff., 231 – *Bundesnotbremse I*; 159, 355 Rn. 110 ff. – *Bundesnotbremse II*; 161, 299 Rn. 155 – *Impfnachweis (COVID-19)*; BVerwG NVwZ 2023, 1326 Rn. 102 – *Treuhandverwaltung nach EnSiG*.

[21] Zur Gewährleistung der IT-Sicherheit als Teilausschnitt der Pflicht des Staates zur Sicherung der Energieversorgung: *Guckelberger*, DVBl 2015, 1213 (1214 f.); *Rath/Ekardt/Schiela*, MMR 2003, 176.

[22] Vgl. allgemein *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 40 f.

Einwirkung auf Software sind also unmittelbare Beeinträchtigungen spezifischer Freiheitsrechte denkbar, so dass auch diese anderen Grundrechte als Ursprung einer staatlichen Schutzpflicht in Betracht kommen.

Ob sich staatliche Schutzpflichten auch allgemein und zentral verankern ließen, das heißt unabhängig von konkreten grundrechtlichen Gewährleistungsbereichen, erscheint zweifelhaft. Mit dieser Frage beschäftigen sich Diskussionen um ein allgemeines Grundrecht auf IT-Sicherheit.[23] Übertragen auf den Gegenstand dieser Untersuchung könnte also nach einem Grundrecht auf sichere Software gefragt werden. Software kommt im grundrechtlichen Koordinatensystem typischerweise ein dienender Charakter zu. Bei ihrer Nutzung handelt es sich um ein Mittel zum Zweck und zwar den Zweck der Grundrechtsausübung, sei es z.B. als Kommunikation mit anderen oder einer beruflichen Tätigkeit.[24] Auch bei der Nutzung von Software handelt es sich typischerweise um eine besondere Form der Grundrechtsausübung. Unter diesen Bedingungen und ohne Anhaltspunkt im Wortlaut der Verfassung ist es nicht gerechtfertigt, ein eigenständiges Grundrecht auf sichere Software anzunehmen. Die Verwendung von Software präsentiert sich vielmehr als eine Art Annex zur Ausübung der in den Grundrechten geregelten Freiheiten.[25]

III. Staatliche Funktionsbedingung als Ursprung einer staatlichen Verantwortung für sichere Software

Daneben gibt es einen weiteren Begründungsstrang für eine staatliche Verantwortung. Denn trotz der Möglichkeit, den Einsatz von Software dem Gewährleistungsgehalt unterschiedlichster Grundrechte zuzuweisen, sind damit nicht alle Einsatzfelder von Software abgedeckt, bei denen über eine staatliche Verantwortung nachgedacht werden kann.

Staatliche Organisationen und Verfahren sind zunehmend digitalisiert und vernetzt – auch wenn sich mitunter der Eindruck einstellt, dieser Prozess könnte noch bedeutend schneller voranschreiten. Entscheidet sich der Staat für eine Digitalisierung von bestimmten Prozessen, kann ihn eine Verantwortung für die Folgen der Digitalisierung treffen.[26] Das Sicherheitsniveau darf nicht wesentlich hinter demjenigen zurückbleiben, das in der „analogen Verwaltung" bestand. Der Staat trägt insofern auch sich selbst und seinen Funktionen gegenüber Verantwortung. Dies ist schon oben angeklungen

[23] *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 43 f.

[24] *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 44.

[25] Vgl. auch *Peuker*, in: Kohtamäki/Peuker (Hrsg.), Die Digitalisierung der öffentlichen Verwaltung, 2023, 159 (161): IT-Sicherheit als „heterogene, komplexe Querschnittsaufgabe".

[26] *Wischmeyer*, in: Hill/Mehde (Hrsg.), Herausforderungen für das Verwaltungsrecht, 2023, 133 (144 ff.) m.w.N. Vgl. zur Gewährleistung von IT-Sicherheit als Bedingung einer E-Government-Nutzungspflicht: *Botta*, NVwZ 2022, 1247.

bei der Darstellung eines Schutzgutes staatlicher Einrichtungen. Der Staat muss gewährleisten, dass seine Wahrnehmung von staatlichen Aufgaben und die Erledigung von Verwaltungsvorgängen frei von Fremdeinwirkungen bleibt. Im Falle des Einsatzes von Software schließt das die Gewährleistung jederzeitiger und nicht korrumpierter Nutzungsmöglichkeit ein.

Für die rechtliche Begründung lässt sich zum einen darauf verweisen, dass die Funktionsfähigkeit der staatlichen Gewaltausübung ein grundlegendes Element der Staatlichkeit an sich ist.[27] Eine souveräne Ausübung staatlicher Gewalt muss in der Lage sein, eigenmächtiges Einwirken Dritter auf die Ausübung zu unterbinden. In der derzeitigen Fassung des BSIG[28] und der BSI-Kritisverordnung[29] findet dies zwar noch keinen direkten Niederschlag; die öffentliche Verwaltung ist nicht als kritische Infrastruktur qualifiziert, obwohl dies in der Sache durchaus nahe gelegen hätte. In der Netz- und Informationssystem (NIS)-2-Richtlinie, die bis zum 17.10.2024 umzusetzen ist und ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen gewährleisten soll, werden aber auch Einrichtungen der öffentlichen Verwaltung auf zentraler und regionaler Ebene ausdrücklich dem Schutzanspruch unterstellt.[30] Die Bedeutung und die Schutzwürdigkeit der öffentlichen Verwaltung ergibt sich indes losgelöst von dieser Richtlinienumsetzung.

Zum anderen kann für die staatliche Funktionsbedingung als Ursprung einer staatlichen Verantwortung an den Charakter berührter Staatsaufgaben angeknüpft werden. Obligatorische Staatsaufgaben und der unveräußerliche Kernbestand staatlicher Aufgaben schließen es ein, dass dem Staat auch effektive Mittel zur erfolgreichen Wahrnehmung solcher Aufgaben zur Verfügung stehen.[31] Dies erfasst auch Software, die im Zusammenhang mit der Aufgabenwahrnehmung eingesetzt wird.[32] Denkbar erscheint dies etwa in Bereichen der Gesetzgebung und Justiz, der Gewährleistung innerer und äußerer Sicherheit, der Strafverfolgung und Finanzverwaltung. Auch in dieser Konstellation kann also festgestellt werden, dass dem Einsatz von Software eine Art Annexfunktion zukommt, hier allerdings zu obligatorischen Staatsaufgaben.

---

[27] Vgl. *Ernst*, Der Grundsatz digitaler Souveränität, 2020, 48 ff.

[28] Gesetz vom 14.8.2009 (BGBl. I S. 2821).

[29] Verordnung vom 22.4.2016 (BGBl. I S. 958).

[30] Art. 2 Abs. 2 lit. f i.V.m. Anhang I Nr. 10, Art. 2 Abs. 5 lit. a Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, 80).

[31] Zum Zusammenhang von IT-Sicherheit und staatlicher Infrastrukturverantwortung vgl. *Peuker*, Verfassungswandel durch Digitalisierung, 2020, 290 ff.

[32] Vgl. zur Datenverarbeitung als integraler Bestandteil oder Annex obligatorischer Staatsaufgaben: *Ernst*, Der Grundsatz digitaler Souveränität, 2020, 27 ff.

IV. Leitbilder der Verantwortungsverteilung zwischen Staat und Gesellschaft

Die Begründung einer staatlichen Verantwortung muss nicht zwangsläufig gleichbedeutend sein mit seiner alleinigen Verantwortung. Vielmehr kann im Ausgangspunkt von einer Mitverantwortung ausgegangen werden, weil neben die staatliche Verantwortung auch eine solche privater Akteure tritt. Dabei sind im Bereich von Software zu verschiedenen gesellschaftlichen Akteuren Verantwortungsverteilungen denkbar.

Eine Verantwortungsverteilung kann zwischen dem Staat und den Bürgerinnen und Bürgern, die als Nutzer auftreten, bestehen. Die Frage nach einer staatlichen Verantwortung provoziert deshalb zugleich die Frage nach dem Nutzerleitbild und der Selbstverantwortung der Nutzerinnen und Nutzer.[33] Die allgemeine Handlungsfreiheit und das allgemeine Persönlichkeitsrecht ermöglichen dem Einzelnen ein selbstbestimmtes Leben und damit auch die Entscheidung, sich zu unterschiedlichsten Zwecken Software zu bedienen. Braucht es deshalb überhaupt einer staatlichen Verantwortung in solchen Fällen, in denen es um Software geht, die selbstbestimmt und aufgrund einer freien Entscheidung von Bürgerinnen und Bürgern genutzt wird, oder erfolgt Softwarenutzung in solchen Fällen ausschließlich eigenverantwortlich?

In der Entscheidung zu IT-Sicherheitslücken geht das Bundesverfassungsgericht implizit davon aus, dass für die Bürgerinnen und Bürger grundsätzlich Selbstschutzmöglichkeiten bestehen; das Gericht nimmt eine besondere Schutzverpflichtung des Staates im konkreten Fall gerade deshalb an, weil den Betroffenen die Selbstschutzmöglichkeiten fehlen.[34] Darin könnte sich ein prinzipieller Vorrang bürgerlicher Selbstschutzmöglichkeiten andeuten, der dann durch eine staatliche Schutzpflicht ergänzt wird, wenn zusätzlich besondere Umstände vorliegen. Ein solcher besonderer Umstand kann – wie im verfassungsgerichtlichen Verfahren – überlegenes staatliches Wissen sein. Denkbar wären aber auch im Einzelfall tatsächlich überlegene staatliche Fähigkeiten und Möglichkeiten oder drohende Gefahren, die nicht nur den einzelnen Nutzer betreffen, sondern auch eine größere Zahl Dritter oder gar das Gemeinwesen. Sollte das Gericht so zu verstehen sein, könnte man die Konturen einer staatlichen Reserveverantwortung im Verhältnis zur bürgerlichen Selbstschutzmöglichkeit darin erblicken. Dagegen spricht allerdings in der Sache, dass der überwiegenden Zahl der Bürgerinnen und Bürger die Fähigkeiten fehlen werden, um im Umgang mit Software selbst Risiken und Gefahren realistisch einschätzen sowie effektive Sicherheitsvorkehrungen treffen zu können.

Die Verantwortung für sichere Software kann daneben mit privaten Akteuren geteilt werden, auch wenn diese nicht als selbstverantwortliche Nutzer auftreten. In erster

---

[33] Zu einem „Leitbild des Durchschnittsnutzers" *Schadel*, Informationsrechte und -pflichten bei Sicherheitslücken im Internet, 2007, 103 ff.

[34] BVerfGE 158, 170 Rn. 40 – *IT-Sicherheitslücken*.

Linie betrifft dies staatlich geschaffene Gewährleistungsansprüche des Zivilrechts, mit denen der Verantwortungsanteil der Entwickler und Vertreiber von Software erfasst wird. Die Einbindung solcher privater Unternehmen, auch soweit diese nicht als Entwickler und Vertreiber von Software auftreten, ist im Modell einer Verantwortungsverteilung grundsätzlich möglich.[35] So werden selbst im Bereich der an sich staatlichen Aufgabe Sicherheit Verantwortungsteilungen durchaus diskutiert, etwa im Hinblick auf die Privatisierung des Maßregelvollzugs oder die Bewachung öffentlicher Einrichtungen.[36] Dabei hat der Staat jedoch Vorkehrungen gegenüber einer Verantwortungsdiffusion zu treffen. Wenn, wie hier, die Verantwortung des Staates auch aus einer grundrechtlichen Schutzpflicht folgt, können gesellschaftliche Akteure nicht undifferenziert in eine Art Verantwortungsgemeinschaft genommen werden.

Hauptsächlich für Bereiche der Daseinsvorsorge und Privatisierung sind aus diesen Gründen bestimmte Leitbilder zur Verantwortungsverteilung und -abschichtung wie Erfüllungs-, Gewährleistungs-, Überwachungs-, Privatisierungsfolgen-, Regulierungs- oder Auffangverantwortung erarbeitet worden. Für den Bereich der Software ist zu berücksichtigen, dass dieser bislang maßgeblich durch Private geprägt worden ist, so dass es für den Staat häufig um einen erstmaligen Zugriff geht.[37] Insbesondere Modelle der Verantwortungsverteilung aus Privatisierungskonstellationen können deshalb nur begrenzt herangezogen werden.

Der konkreten Verantwortungsteilung in einem mehrpoligen Rechtsverhältnis, wie es dem tatsächlichen Umfeld von Softwaresicherheit entspricht, setzt die Verfassung durch das Unter- und Übermaßverbot nur äußerste Grenzen.[38] Eine Schutzpflicht, die wegen einer geänderten Bedrohungslage neu entsteht, kann vorläufig schon dadurch erfüllt werden, dass der Gesetzgeber die auftretende Konfliktlage überhaupt normiert und dabei nicht gänzlich ungeeignete Maßnahmen trifft. Dem Gesetzgeber kommt ein Einschätzungs-, Wertungs- und Gestaltungsspielraum zu, wenn er darüber entscheidet, ob, mit welchem Schutzniveau und auf welche Weise Gefahrensituationen begegnet werden soll.[39] Es besteht grundsätzlich keine Verpflichtung, öffentliche Aufgaben nur

[35] Vgl. z.B. zur Erfassung von Software durch eine Erweiterung des Anwendungsbereichs des Produktsicherheitsrechts: *Bäumerich*, DVBl 2019, 219.

[36] Vgl. BVerfGE 130, 76 (111 ff.) – *Privatisierung des Maßregelvollzugs*; BVerwGE 81, 185 ff. – *Bewaffneter Werkschutz im Kernkraftwerk*; *Bracher*, Gefahrenabwehr durch Private, 1987, insb. 179: kein staatliches Monopol der Gefahrenabwehr. Vgl. zur Wahrnehmung militärischer Wachaufgaben der Bundeswehr durch Zivilisten § 1 Abs. 3 des Gesetzes über die Anwendung unmittelbaren Zwanges und die Ausübung besonderer Befugnisse durch Soldaten der Bundeswehr und verbündeter Streitkräfte sowie zivile Wachpersonen v. 12.8.1965 (BGBl. I S. 796) und dazu die verfassungsrechtliche Bewertung durch *Gramm*, VerwArch 90 (1999), 329 (355 ff.).

[37] Vgl. allgemein *Schmidt-Preuß*, in: HVwR I, 2021, § 26 Rn. 12 m.w.N.: Erstmaliger Zugriff statt Rückholung.

[38] Statt vieler BVerfGE 121, 317 (356 f.) m.w.N. – *Nichtraucherschutz*.

[39] BVerfGE 121, 317 (356).

mit öffentlichen Mitteln zu erfüllen,[40] zumal für die IT- und Telekommunikationsunternehmen als Kehrseite ihrer erheblichen Profitchancen eine besondere Verantwortungsnähe begründet werden kann.[41] Dabei muss der Gesetzgeber aber erkennbare strukturelle Probleme berücksichtigen; im Falle der Softwaresicherheit wäre daran zu denken, dass private Diensteanbieter „unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben".[42]

In einem Bereich wie dem der Softwaresicherheit muss die Lage weiter im Wege eines dynamischen Grundrechtsschutzes[43] und einer Beobachtungsverantwortung[44] durchgängig überwacht und gegebenenfalls angepasst werden.[45] Bei einer unterlassenen Anpassung wird man allerdings erst dann von einem Verfassungsverstoß sprechen können, wenn die ursprüngliche Regelung mittlerweile verfassungsrechtlich untragbar ist, weil sich Verhältnisse geändert haben, der Gesetzgeber aber dennoch untätig geblieben ist oder nur Anpassungen vorgenommen hat, die offensichtlich fehlsam sind.[46]

Im Bereich der Softwaresicherheit kann zur Erfüllung der Schutzpflicht nicht auf das historische Leitbild umfassender staatlicher Erfüllungsverantwortung als „Goldstandard" zurückgegriffen werden. Es erscheint rechtlich nicht angezeigt, eine Zentralisierung oder Monopolisierung der Gewährleistung von Softwaresicherheit beim Staat anzustreben – faktisch ist dies ohnehin fernliegend.[47] Bei der Vorratsdatenspeicherung hatte das Bundesverfassungsgericht den Umstand, dass die Daten grundsätzlich bei privaten Diensteanbietern verbleiben, in der Abwägung *zugunsten* der Verfassungsmäßigkeit berücksichtigt.[48] Angesichts der tatsächlichen Ressourcen des Staates, aber auch seiner Fähigkeiten im Vergleich zu privaten Akteuren – hier ist insbesondere an die je-

[40] Vgl. zur Frage, ob die Eigenerfüllung durch den Staat gegenüber einer Belastung eines Privaten als mildere Maßnahme anzusehen ist (verneinend): BVerfGE 109, 64 (86); 113, 167 (259); 116, 96 (127); 125, 260 (360).

[41] BVerfGE 125, 260 (362) – *Vorratsdatenspeicherung*.

[42] BVerfGE 125, 260 (325) – *Vorratsdatenspeicherung*.

[43] Grundlegend BVerfGE 49, 89 (5. LS und 137, 140) – *Kalkar*.

[44] *Franzius*, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts I, 3. Aufl. 2022, § 4 Rn. 81 f. m.w.N.

[45] Vgl. die Begründung zum zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, BT-Drs. 19/26106, 1, 30: „Insgesamt ist Cyber-Sicherheit nicht statisch, ein aktuelles Schutzniveau ist daher kein Garant für eine erfolgreiche Abwehr der Angriffe von morgen. Daher bedarf es einer ständigen Anpassung und Weiterentwicklung der Schutzmechanismen und der Abwehrstrategien." Vgl. auch zum Datenschutz und dem Digitalwirtschaftsrecht als Referenzgebiete für Überwachung: *Huber*, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts II, 3. Aufl. 2022, § 43 Rn. 62 f.

[46] So zuletzt etwa BVerfG (K) NJW 2016, 1716 Rn. 19 m.w.N. – *Pflegenotstand*.

[47] Vgl. *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 49.

[48] BVerfGE 125, 260 (360): „Eine Übermittlung aller Verbindungsdaten an den Staat, damit dieser die Speicherung selbst vornimmt, scheidet schon wegen der damit verbundenen Risiken sowohl für den Schutz des Telekommunikationsgeheimnisses als auch für die Sicherheit und Vollständigkeit der Daten aus."

weiligen Entwickler einer Software zu denken –, dürfte einer Schutzpflicht nicht in ausreichendem Maße Genüge getan werden, wenn der Staat private Akteure von dieser Aufgabe ausschließt. Insbesondere die bei Privaten vorhandenen Fähigkeiten sind im Rahmen einer Verantwortungsverteilung zu berücksichtigen.

V. Sichere Software als Abwägungsentscheidung und entgegenstehende Rechtspositionen

Für eine konkrete Aktualisierung staatlicher Verantwortung können grundsätzliche Strukturen und Wertungen herangezogen werden. Das Ausmaß an Sicherheit, das gewährleistet werden kann, hängt ab von dem Aufwand, den Kosten und dem Einsatz, der aufgewendet wird. Nur der Vollständigkeit halber soll erwähnt werden, dass auch im optimalen Fall eine hundertprozentige Sicherheit für Software realistisch nicht zu erreichen sein dürfte. Das Sicherheitsniveau – und damit die Frage, in welchem Ausmaß der Staat seiner Verantwortung nachkommt – ist damit eine Frage der Abwägung. Dies gilt insbesondere angesichts der Begründung als grundrechtliche Schutzpflicht.[49] Nichts anderes gilt, wenn eine staatliche Verantwortung aus der Funktionsfähigkeit staatlicher Gewaltausübung oder der Wahrnehmung originärer Staatsaufgaben folgt. Auch in diesen Konstellationen können kollidierende Verfassungsgüter nicht ausgeblendet werden.

Je nach Kontext bestehen unterschiedliche Rechtspositionen, die dem Ziel einer sicheren Software entgegenstehen können. Oben schon angesprochen wurden die Kosten und der dafür notwendige Aufwand.[50] Dabei ist zu berücksichtigen, dass das Verhältnis von Kosten und Sicherheit nicht zwingend allgemeingültig bestimmt werden kann. Unter Berücksichtigung der unternehmerischen Freiheit der Softwareentwickler sind durchaus ganz unterschiedliche Bewertungen denkbar, weil eine Software etwa gewinnbringend zu einem bestimmten Preis angeboten werden soll. Auch der Aufwand für die Nutzerinnen und Nutzer oder die Leistungsfähigkeit einer Software kann in einem Spannungsverhältnis zum Sicherheitsniveau stehen.

Von erheblicher Bedeutung für die staatliche Verantwortung ist der Verwendungskontext einer bestimmten Software, auch wenn sich dies natürlich häufig nicht auf einzelne Einsatzfelder begrenzen lässt. Dies zeigt sich zum Beispiel an gängigen Betriebssystemen, die in ganz unterschiedlichen Zusammenhängen zum Einsatz kommen. Angesichts der Begründungsansätze für eine staatliche Verantwortung lässt sich für eine Abwägung zum einen auf die Bedeutung für den Einzelnen und zum anderen auf die Bedeutung für das Gemeinwesen abstellen. Letzteres weist eine breite Überschneidung

[49] Vgl. BVerfGE 121, 317 (356 f.) zum Spielraum des Gesetzgebers bei der Erfüllung von Schutzpflichten.

[50] Vgl. Art. 32 Abs. 1 Datenschutz-Grundverordnung, der bestimmt, dass die datenschutzrechtlich gebotenen technischen und organisatorischen Maßnahmen neben dem Stand der Technik auch von den Implementierungskosten abhängen.

mit den klassischen Einrichtungen der Daseinsvorsorge auf und wird mit unterschiedlichen Begrifflichkeiten in verschiedenen Regelungswerken aufgegriffen. Zum Beispiel knüpfen das BSIG und die BSI-Kritisverordnung an die Eigenschaft als Betreiber „Kritischer Infrastrukturen“[51] und als „Unternehmen im besonderen öffentlichen Interesse“ [52] an, die sog. NIS-Richtlinie spricht von „Betreibern wesentlicher Dienste“[53] und branchenspezifisch finden sich außerdem weitere Regelungen, etwa für die Gesundheitsversorgung durch Vertragsärzte und in Krankenhäusern im SGB V[54] und für Kritische Infrastrukturen der Energieversorgung im Energiewirtschaftsgesetz[55].

Schließlich ist es auch denkbar, dass staatliche Interessen der Softwaresicherheit entgegenstehen können. Das Bundesverfassungsgericht hatte in seiner Entscheidung zur Ausnutzung von IT-Sicherheitslücken durch die Sicherheitsbehörden, wenn diese zwar den Sicherheitsbehörden, nicht aber den Nutzern oder den Herstellern bekannt sind, ebenfalls die Notwendigkeit einer Abwägung betont.[56] Dabei hat es den Behörden auferlegt, auch die Gefahr einer weiteren Verbreitung der Kenntnis von der Sicherheitslücke zu ermitteln und ins Verhältnis zu setzen mit dem Nutzen einer behördlichen Infiltration. Ob damit jedoch einer staatlichen Verantwortung hinreichend Rechnung getragen wird, erscheint fraglich. Das Bundesverfassungsgericht geht zwar auf verschiedene Risiken ein, die mit dem Ausnutzen von Sicherheitslücken verbunden sein können. Dabei dürften aber zusätzliche Verbreitungs- und Ausnutzungsrisiken bestehen, die nicht eigenständig betrachtet werden.[57] Die vom Gericht geforderte Ermittlung, wie verbreitet eine Sicherheitslücke ist, dürfte häufig schwer sein, weil ihr Ausnutzen typischerweise darauf beruht, dass dies im Geheimen geschieht.[58] Auch etwa mit der Frage, welche Bedeutung der Verbreitung der fehlerbehafteten Software zukommt und in welchen Bereichen sie eingesetzt wird, beschäftigt sich das Gericht nicht näher. Dies ist umso misslicher, weil für die Sicherheit von Software Aspekte in erheblicher Vielfalt bestehen, die sich für eine Abwägung auswirken können. Zugleich besteht aber in der Praxis mitunter die Tendenz, sich sehr stark am Wortlaut einer Entscheidung zu halten. In welchem Ausmaß die vom Gericht lediglich abstrakt angedeuteten Auslegungsspielräume dann tatsächlich genutzt werden, erscheint deshalb nicht sicher. Insgesamt erscheint es deshalb zweifelhaft, ob die vom Bundesverfassungsgericht vorgenommene

[51] § 2 Abs. 10, § 10 Abs. 1 BSIG i.V.m. §§ 1 ff. BSI-Kritisverordnung.

[52] § 2 Abs. 14, § 8f BSIG.

[53] Art. 4 Nr. 4, Art. 5 i.V.m. Anhang II, Art. 14 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, 1).

[54] §§ 75b, 75c SGB V.

[55] § 11 Abs. 1b–1f Energiewirtschaftsgesetz.

[56] BVerfGE 158, 170 Rn. 44 – *IT-Sicherheitslücken*.

[57] *Wischmeyer*, Informationssicherheit, 2023, 289 ff.; vgl. *ders*., in: Hill/Mehde (Hrsg.), Herausforderungen für das Verwaltungsrecht, 2023, 133 (147).

[58] Zur Unterscheidung zwischen dem Ausnutzen einerseits bekannter und andererseits unbekannter Sicherheitslücken vgl. *Wischmeyer*, Informationssicherheit, 2023, 284.

Abwägung angesichts der Unterschiedlichkeit der tatsächlich relevanten Kriterien eine angemessene Lösung darstellt; zumindest wäre es wünschenswert gewesen, wenn das Gericht ausführlicher zu den Abwägungskriterien Stellung genommen und deren Bedeutung auch stärker gewichtet hätte.

C. Kategorien der Verantwortungswahrnehmung

Im Folgenden sollen nun Regelungen, mit denen der Staat seine Verantwortung wahrnimmt, grob kategorisiert werden. Dazu soll zwischen informatorischen Maßnahmen, Vorsorgemaßnahmen sowie Gefahrenabwehrmaßnahmen und repressiven Maßnahmen unterschieden werden.

Auf drei Punkte soll eingangs kurz hingewiesen werden: Mittlerweile besteht eine erhebliche Vielfalt an gesetzlichen Regeln, die (auch) zum Gegenstand haben, Softwaresicherheit aufrechtzuhalten. Die folgenden Ausführungen können deshalb nicht auf jede einzelne Vorschrift eingehen, sondern konzentrieren sich auf exemplarische Strukturen und typische Regelungsmechanismen. Außerdem wird nicht gesondert auf zivilrechtliche Regelungen eingegangen, auch wenn diese als staatlich gesetztes Recht Ausdruck einer staatlichen Verantwortung sind.[59] Schließlich fällt bei einer Sichtung der unterschiedlichen Regelungen auf, dass der Begriff „Software“ durch den Normgeber regelmäßig nicht aufgegriffen wird. Stattdessen wird begrifflich auf Informationstechnik, technisch organisatorische Maßnahmen oder zum Beispiel Cybersecurity Bezug genommen. Typischerweise erfassen diese Regelungsregime aber sowohl Hard- wie Software,[60] weshalb diese begriffliche Diskrepanz nicht weiter vertieft werden soll.

I. Informatorische Maßnahmen

Ein erster Normkomplex zielt auf Informationen über Softwaresicherheit ab. Abgedeckt davon sind Rechtsgrundlagen, die das Erheben von Informationen ermöglichen. So regelt § 4a BSIG die selbständige Kontrolle der Sicherheit von Kommunikationstechnik durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und § 4b die Entgegennahme von Meldungen. In vielen Situationen ist es aber nicht möglich, selbständig alle notwendigen Informationen zu erhalten. Für den Fall sieht der Gesetzgeber Meldeverpflichtungen vor. § 8f Abs. 7 BSIG verpflichtet Unternehmen im besonderen öffentlichen Interesse Störungen zu melden, § 8b Abs. 4 und § 8c Abs. 3 BSIG enthalten Meldepflichten bei Sicherheitsvorfällen und § 9b BSIG regelt etwa eine Anzeigepflicht beim Einsatz kritischer Komponenten bzw. eine Garantieerklärung.

[59] Vgl. *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 49.
[60] Kipker/Reusch/Ritter/*Ritter*, Recht der Informationssicherheit, 2023, BSIG § 2 Rn. 2.

Solche Meldepflichten finden sich auch im Atomgesetz für die Betreiber kerntechnischer Anlagen oder im Telekommunikationsgesetz (TKG) für die Betreiber öffentlicher Telekommunikationsnetze.[61] Diese Informationserhebungsregelungen und Meldepflichten verfolgen den Zweck, das für die Wahrnehmung der staatlichen Verantwortung notwendige Wissen zu generieren.[62] Bei diesen Beobachtungsstrukturen handelt es sich um eine Vorbedingung eines effektiven Rechtsgüterschutzes.

Informatorische Maßnahmen können auch darauf ausgerichtet sein, diesen Rechtsgüterschutz schon selbst sicherzustellen. § 7 BSIG enthält die Befugnis der Behörde, öffentlich zu warnen und § 9c Abs. 1 BSIG regelt die Verbraucheraufklärung mittels eines Sicherheitskennzeichens. Vergleichbar, aber unter Einbeziehung Dritter, bestimmt § 168 Abs. 6 TKG im Falle eines Sicherheitsvorfalls eine Informationsverpflichtung des Netzbetreibers gegenüber den Nutzern. Die staatliche Schutzverantwortung wird dann nicht durch eigene Maßnahmen gegenüber der Gefahr realisiert, sondern indem die Nutzerinnen und Nutzer in die Lage versetzt werden, sich effektiv selbst schützen zu können.

Jüngst sorgte die öffentliche Warnung des BSI vor einer Virenschutzsoftware, gestützt auf § 7 BSIG, für Aufmerksamkeit. Maßstab für eine solche Warnung ist das Vorliegen hinreichender Anhaltspunkte, dass von einer Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen. Das Oberverwaltungsgericht Münster bestätigte die Rechtmäßigkeit der Warnung, allerdings nicht unter Verweis auf unbeabsichtigte technische Schwachstellen oder Fehler in der Software.[63] Maßgeblich war vielmehr, wie auch schon für das BSI und die Vorinstanz, dass Virenschutzsoftware typischerweise funktionsbedingt über weitreichende Systemberechtigungen verfügt und eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten muss.[64] Würden diese Funktionen ausgenutzt werden, könnten sich Dritte gegen den Willen der Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen. Dieses Risiko sah das Oberverwaltungsgericht Münster als gegeben an, weil sich der Hersteller der Virenschutzsoftware auch nach dem russischen Angriff auf die Ukraine 2022 nach wie vor mit wesentlichen Unternehmensstrukturen und -fähigkeiten im Einflussbereich des russischen Regimes befindet. Es lägen demnach insgesamt hinreichende Anhaltspunkte vor, dass die Virenschutzsoftware durch das russische Regime für Cyberangriffe missbraucht werden könnte – möglicherweise ohne Zutun des Herstellers, vielleicht aber auch, indem der Hersteller selbst zu einer Ausnutzung genötigt wird.

[61] Siehe § 44b Atomgesetz und § 168 TKG.
[62] Vgl. *Leisterer*, Internetsicherheit in Europa, 2018, 31 ff. zur Netz- und Informationssicherheit.
[63] OVG Münster NJW 2022, 1547.
[64] Zum Folgenden OVG Münster NJW 2022, 1547 Rn. 27 ff.

Diese Entscheidung ist im Ergebnis und in der Bewertung der tatsächlichen Lage durchaus nachvollziehbar. Fraglich ist aber, ob das gerichtliche Vorgehen auch dem gesetzlichen Verständnis der Sicherheitslücke nach dem BSIG entspricht. Die besonderen technischen Eigenschaften einer Virenschutzsoftware sind von den Entwicklern als wesentliches Funktionsmerkmal gewollt und notwendig. Zwar ist der gesetzliche Begriff der Sicherheitslücke in § 2 Abs. 6 BSIG weit zu verstehen[65] und der Gesetzeswortlaut stellt nur auf „Eigenschaften" einer Software ab, nicht aber, ob diese intendiert sind oder mit welcher Motivation sie verwendet werden.[66] Doch mit diesem Verständnis verliert die Schwelle zwischen technischen und organisatorischen Maßnahmen, zwischen unerwünschten technischen Gegebenheiten auf der einen Seite und unerwünschten Nutzern oder unerwünschten Absichten auf der anderen Seite an Konturen. Für die Bestimmung der Sicherheit würde damit der Umgang mit Software im Vordergrund stehen, nicht aber die Software selbst. Dass dahinter zwei grundsätzlich unterschiedliche Sicherheitsverständnisse stehen, konnte oben aufgezeigt werden. Bei diesem Vorgehen ist auch schon die Eingabeaufforderung der Kontoinformationen zur Nutzung eines Betriebssystems eine Sicherheitslücke – immerhin könnte auch jemand Unbefugtes die korrekte Nutzerkennung und das dazugehörige Passwort eingeben. Alles, was missbraucht werden kann, wäre auch eine Sicherheitslücke im Sinne des Gesetzes. Für das behördliche Instrumentarium käme es dann allein darauf an, ob tatsächliche Anhaltspunkte für einen Missbrauch bestehen.[67] Aus Gründen der Rechtssicherheit wäre es wünschenswert, das Merkmal der Sicherheitslücken und ihr Ausnutzen schärfer zu konturieren. Dabei erscheint es keinesfalls ausgeschlossen, dass es eine staatliche Verantwortung für Softwaresicherheit notwendig macht, auch die organisatorischen, persönlichen, gesellschaftlichen oder politischen Umstände zu berücksichtigen, denen Hersteller oder Dritte ausgesetzt sind.

II. Gefahrenvorsorge und Anforderungen an Hersteller

Entsprechend dem Verantwortungsansatz, ex-ante für das Bewahren eines bestimmten Zustands einzutreten, findet sich eine Fülle gesetzlicher Regeln, die bestimmte Anforderungen an Softwarehersteller beinhalten und damit der Gefahrenvorsorge dienen.[68] Das prägnanteste Beispiel für diese Kategorie bilden Regeln, die zur Berücksichtigung des Stands der Technik verpflichten, wie zum Beispiel § 165 TKG für Telekommunikationsnetz- und -dienstbetreiber oder § 75b SGB V für Krankenhäuser. Im BSIG findet sich dieser Passus in einer Reihe von Vorschriften, wie etwa § 8a für kritische Infrastrukturen, § 8c für Anbieter digitaler Dienste oder § 8f für Unternehmen im besonderen öffentlichen Interesse.

---

[65] Kipker/Reusch/Ritter/*Ritter*, Recht der Informationssicherheit, 2023, BISG § 2 Rn. 16.
[66] Siehe aber BT-Drs. 16/11967, 12 („unerwünschte Eigenschaften").
[67] *Dittrich*, NJW 2022, 2971 Rn. 12 ff.
[68] Vgl. *Poscher/Lassahn*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 46.

Der „Stand der Technik" wird allgemein zwischen dem anforderungsvolleren „Stand der Wissenschaft und Forschung" sowie den „allgemein anerkannten Regeln der Technik" eingeordnet.[69] Unmittelbar mit dieser Formulierung sind jedoch keine konkreten Vorgaben für Sicherheitsvorkehrungen verbunden. Das Merkmal ist entwicklungsoffen, um eine kontinuierliche Anpassung an die tatsächliche Lage zu ermöglichen, und muss typischerweise durch Behörden oder unter Zuhilfenahme Privater konkretisiert werden; nach § 8a Abs. 2 BSIG erfolgt dies z.B. durch Einbeziehung der Betreiber kritischer Infrastrukturen und ihrer Branchenverbände. Mit dem Rückgriff auf dieses Merkmal hat der Gesetzgeber in solchen Fällen deshalb die Verantwortungsverteilung mit Privaten aktualisiert, die in die Erstellung der konkreten Anforderungen an die Sicherheit von Software eingebunden sind. Auf einer äußerst abstrakten und rudimentären Ebene hat der Gesetzgeber durch die Einordnung des Stands der Technik zu vergleichbaren Instituten auch für die Abwägung zwischen dem zu betreibenden Aufwand sowie den Kosten und dem Sicherheitsniveau eine pauschale Richtung vorgegeben. Damit verwandt sind solche Vorschriften, die zwar nicht auf das Instrument „Stand der Technik" abstellen, aber in ähnlicher Art und Weise Sicherheitsanforderungen formulieren. So erarbeitet nach § 8 Abs. 1 BSIG das BSI Mindeststandards für die Sicherheit der Informationstechnik des Bundes. § 11 Energiewirtschaftsgesetz enthält einen Katalog von Sicherheitsanforderungen für den Betrieb von Energieversorgungsnetzen ebenso wie § 167 Abs. 1 TKG für Telekommunikations- und Datenverarbeitungssysteme. Eine konkrete Vorgabe findet sich demgegenüber z.B. in § 1 Abs. 24, § 55 Zahlungsdiensteaufsichtsgesetz. Damit ist eine starke Kundenauthentifizierung unter Verwendung zweier voneinander unabhängiger Elemente zum Beispiel beim Online-Banking gefordert.

III. Maßnahmen zur Abwehr konkreter Gefahren und repressive Maßnahmen

Behördliche Befugnisse zur Abwehr konkreter Gefahren finden sich in §§ 7c und 7d BSIG. Die Maßnahmenstruktur nimmt Anleihen beim allgemeinen Gefahrenabwehrrecht und verlangt vor allem eine konkrete erhebliche Gefahr. Eine vergleichbare Befugnis findet sich in § 165 Abs. 8 TKG.

Im Übrigen ist es nicht ausgeschlossen, dass auch die allgemeinen Polizei- und Ordnungsbehörden zur Abwehr softwarebezogener Gefahren zuständig sind,[70] wenngleich regelmäßig die notwendige Ausstattung dafür fehlen wird. Repressive Maßnahmen in

[69] *Skierka*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 8 Rn. 10; vgl. BVerfGE 49, 89 (135 ff.); allgemein *Haffner*, Kosten-Nutzen-Abwägungen im Sicherheitsrecht, 2016, 145 ff.; *Knopp*, DuD 2017, 663; *Hwang*, Der Staat 49 (2010), 456.

[70] Dazu bereits der Nachw. in Fn. 8 sowie *Bäcker/Golla*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 18 Rn. 53; *Golla*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. I, Rn. 654.

Form von Geldbußen finden in § 14 BSIG oder in § 228 TKG sowie etwa in den §§ 202a-202d StGB oder dem §§ 268 ff. StGB. Im Vergleich zeigt sich aber, dass die Maßnahmen zur Abwehr konkreter Gefahren und repressive Maßnahmen deutlich weniger ausdifferenziert sind als die Vorfeldmaßnahmen.

D. Fazit und Andeutungen von Grundstrukturen

Die Entscheidung über eine staatliche Verantwortung für sichere Software ist eine multifaktorielle Entscheidung. Dabei spielen unter anderem das Ausmaß drohender Gefahren, der Verwendungszweck der Software und ihre Bedeutung für das Gemeinwesen, ihre Verbreitung, die Fähigkeiten ihrer Nutzer, die technischen Möglichkeiten sowie der Aufwand und die Kosten für eine Verbesserung der Sicherheit eine maßgebliche Rolle. Die Wahrnehmung einer staatlichen Verantwortung ist deshalb eine Abwägungsentscheidung. Eine rechtliche Grundlage findet diese Verantwortung sowohl in grundrechtlichen Schutzpflichten als auch in der Funktionsfähigkeit der staatlichen Gewaltausübung als grundlegendes Element der Staatlichkeit. Die grundrechtliche Anbindung ist dabei nicht auf Art. 10 Abs. 1 GG oder das IT-Grundrecht beschränkt. Je nach Kontext kommen dafür potenziell auch andere Grundrechte in Betracht. Es erscheint sinnvoll, die traditionell bestehende Verbindung zum Persönlichkeitsrecht und dem Datenschutz, wie sie insbesondere im IT-Grundrecht zum Ausdruck kommt, zurückzunehmen, und stattdessen die Annexfunktion zu einzelnen Freiheitsrechten zu betonen. Softwarenutzung kann als Ausübungsmodalität grundrechtlicher Freiheiten angesehen werden. Für eine Ableitung aus der staatlichen Funktionsfähigkeit kann es etwa auf originäre Staatsaufgaben ankommen. Die Verantwortung für Software stellt sich auch in dieser Hinsicht als Annex dar, und zwar zur konkreten staatlichen Aufgabe. Eine Verantwortung, die auf diesen Pfeilern beruht, bleibt aber regelmäßig keine ausschließliche staatliche Verantwortung, sondern trifft typischerweise auf die Verantwortung Privater. Dem Gesetzgeber stehen zur Ausgestaltung dieser Gemengelage unterschiedlich abgestufte Regelungen zur Verfügung. Ein Schwerpunkt findet sich dabei in Informationsregelungen und Vorsorgemaßnahmen, die an Software bestimmte Anforderungen stellen.

Staatliche Nutzung von IT-Sicherheitslücken – Grundzüge des staatlichen Schwachstellenmanagements

Thomas Wischmeyer

A. Einführung

IT-Sicherheit ist die Achillesferse der Digitalisierung. Vom Einsatz elektronischer Akten in der Verwaltung bis zur Nutzung generativer künstlicher Intelligenz: Digitaler Fortschritt ohne hinreichende IT-Sicherheit ist und bleibt prekär. Zu Recht werden daher gegenwärtig erhebliche politische, ökonomische, technische und auch rechtliche Ressourcen mobilisiert, um Sicherheitslücken vorzubeugen, diese zu schließen oder jedenfalls das Risiko einer Nutzung durch Unbefugte zu minimieren.

Gleichzeitig wecken Sicherheitslücken Begehrlichkeiten bei allen Akteuren, für die der Zugang zu nicht öffentlich verfügbaren Informationen oder die Möglichkeit zur Manipulation von IT-Systemen strategische Vorteile verspricht. Neben privaten Hackern, Hacktivisten und Kriminellen treten dabei zunehmend auch staatliche Stellen als Produzenten und Nutznießer von Cyber-Unsicherheit auf.[1] Überall dort, wo IT-Sicherheit mit der Verfolgung staatlicher Interessen kollidiert, steht im Raum, dass der Staat erstere opfert, um letztere zu realisieren. Dass hier ein enormes Missbrauchspotenzial besteht, liegt auf der Hand. So hat der Pegasus-Untersuchungsausschuss des Europäischen Parlaments im Jahr 2022 aufgearbeitet, dass staatliche Akteure in Polen, Spanien, Zypern, Griechenland, Ungarn und möglicherweise auch in weiteren Mitgliedstaaten der Union Endgeräte von Oppositionspolitikern, Journalisten und deren Angehörigen mit hochpotenter Spionagesoftware infiltriert haben.[2] Dabei wurden Sicherheitslücken der Systeme ausgenutzt, um einen umfassenden Zugriff auf alle mit Hilfe des Geräts ausgetauschten Informationen zu erlangen. Auch Ende-zu-Ende-Verschlüsselung der eigenen Kommunikation bot keinen Schutz. Selbst der Zugriff auf die Kamera und das

[1] *Finnemore/Hollis*, AJIL 110 (2016), 425 (434 f.).

[2] *Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware*, Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22.5.2023, A9-0189/2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf; *European Parliament*, Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 15.6.2023, 2023/2500(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html (letzter Zugriff für alle Internetquellen: 26.10.2023).

Mikrofon der Endgeräte war möglich. Im Falle Polens ist eine Untersuchungskommission des polnischen Senats im September 2023 zum Schluss gekommen, dass das von Regierungsseite verantwortete Eindringen in das Telefon des Wahlkampfleiters der Opposition und die anschließende Veröffentlichung der auf diese Weise abgeschöpften und zusätzlich manipulierten Daten die Fairness der Wahlen von 2019 erheblich beeinträchtigt haben.[3]

Viele Details, auch technischer Natur, liegen im Fall Pegasus nach wie vor im Dunkeln. Doch es kann als gesichert gelten, dass Regierungen, Geheimdienste oder Ermittlungsbehörden in zahlreichen Ländern heute mehr oder weniger routinemäßig IT-Sicherheitslücken nutzen und hierbei teils intensiv mit privaten Herstellern spezieller Software kooperieren.[4] Dies ist nicht nur mit Blick auf die Privatsphäre der Betroffenen problematisch, sondern auch schwer mit den parallelen staatlichen Bemühungen um eine Stärkung der IT-Sicherheit vereinbar. Deutschland selbst ist insoweit zwar bislang von größeren politischen Skandalen verschont geblieben. Doch auch hier nutzen Behörden IT-Sicherheitslücken, ohne dass das Risiko eines Missbrauchs sicher ausgeschlossen werden kann.[5] Ungeachtet der Missbrauchsmöglichkeit stellt sich zudem die grundlegende Frage, ob staatliche Stellen IT-Sicherheitslücken überhaupt für eigene Zwecke verwenden sollten oder ob (verfassungsrechtliche) Gründe dagegensprechen, dem Staat dieses Mittel an die Hand zu geben. Die folgenden Ausführungen nähern sich dieser Frage in drei Schritten.

Zunächst wird das Problem der staatlichen Nutzung von IT-Sicherheitslücken in den Kontext der staatlichen Verantwortung für die Informationssicherheit eingeordnet. Diese staatliche Verantwortung geht nicht in der Pflicht auf, unverhältnismäßige Überwachung zu unterlassen, sondern ist wesentlich breiter verfassungsrechtlich fundiert (B.). Anschließend sind die informationssicherheitsspezifischen Risiken des staatlichen Umgangs mit IT-Sicherheitslücken präzise zu bestimmen: Was ist, über die Bedrohung der Privatheit hinaus, zu bedenken, wenn der Staat IT-Sicherheitslücken selbst nutzt, statt sich bedingungslos für ihre Schließung einzusetzen? Hierbei ist auch

[3] Vgl. die Zusammenfassung des polnischen Berichts vom 6.9.2023 bei *Pitz*, Überwachung mit Pegasus ist illegal, 11.9.2023, https://netzpolitik.org/2023/polnischer-senat-ueberwachung-mit-pegasus-ist-illegal/.

[4] Laut Aussagen eines Firmenvertreters im EU-Untersuchungsausschuss wurde allein die Spähsoftware Pegasus des israelischen Unternehmens NSO von 14 EU-Mitgliedstaaten eingesetzt (2022: von 12), die hiermit „etwa 12.000 bis 13.000 Ziele" pro Jahr angreifen, vgl. *Meister*, Staatstrojaner Pegasus wird alle 40 Minuten eingesetzt, 22.06.2022, https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/.

[5] Dass deutsche Sicherheitsbehörden jedenfalls in der Vergangenheit Produkte von NSO genutzt haben, ist offiziell nur indirekt bestätigt worden, gilt jedoch allgemein als sicher, vgl. auch *Committee of Inquiry* (Fn. 2), Rn. 365, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf; zu aktuellen Informationszugangsbegehren siehe *Meister*, Wir verklagen das BKA, 27.9.2023, https://netzpolitik.org/2023/staatstrojaner-pegasus-wir-verklagen-das-bka-zum-dritten-mal/.

auf jüngere Entscheidungen des BVerfG einzugehen. Dieses ist in mehreren Verfassungsbeschwerden zur sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) auf die Risiken der staatlichen Nutzung von IT-Sicherheitslücken hingewiesen worden, ist aber in eine ernsthafte Auseinandersetzung mit diesen Risiken bisher nicht eingetreten. Diese Zurückhaltung des Gerichts sollte den Gesetzgeber jedoch nicht davon entlasten, nach einer angemessenen Strategie zur rechtsstaatlichen Einhegung und Minimierung dieser Risiken zu suchen (C.). Wie eine solche Strategie aussehen kann, wird im letzten Teil entwickelt, der der Ausarbeitung von Grundzügen eines staatlichen Schwachstellenmanagements, also von Regeln zum Umgang staatlicher Stellen mit ihnen bekannt gewordenen IT-Sicherheitslücken, gewidmet ist (D.).

B. Der Staat als Garant der Informationssicherheit

Der Fall Pegasus zeigt, dass sich die Öffentlichkeit besonders für jene staatlichen Maßnahmen interessiert, die die Schutzziele der Informationssicherheit kompromittieren. Das ist jedoch nur die eine Seite der Medaille. Wie angedeutet bemühen sich zahlreiche Staaten in den letzten Jahren mit hohem Einsatz um eine Verbesserung der IT-Sicherheitslage und versuchen insofern, ihrer Verantwortung für die Gewährleistung von Informationssicherheit nachzukommen. Die Reichweite dieser Verantwortung orientiert sich am Umfang der Aufgabe. Im vorliegenden Rahmen kann das regulatorische Informationssicherheitsproblem nicht detailliert beschrieben, sondern nur in seinen – sehr weiten – Umrissen skizziert werden (I.). Diese Skizze dient primär dazu, der verfassungsrechtlichen Verantwortung des Staates in Sachen Informationssicherheit in tatsächlicher Hinsicht Konturen zu verleihen (II.).

I. Die Komplexität der Aufgabe Informationssicherheit

Aus technischer Sicht ist die Gewährleistung von IT-, Informations- bzw. Cyber-Sicherheit komplex.[6] Denn Sicherheitslücken bzw. Schwachstellen finden sich in unserer

[6] Zu den verschiedenen Begrifflichkeiten, den damit je verbundenen Konnotationen sowie insgesamt zu den folgenden Abschnitten ausführlich *Wischmeyer*, Informationssicherheit, 2023, S. 26 ff., 188 ff. (open access unter: https://www.mohrsiebeck.com/buch/informationssicherheit-9783161620607).

digitalen Gegenwart allerorten.[7] Für eine erste Orientierung bietet es sich an, durchaus idealtypisch drei Problemebenen zu unterscheiden.[8]

Die *erste* ist die Ebene des System- und Netzwerkschutzes: Welche Risiken der Betrieb eines (heute in der Regel vernetzten) IT-Systems begründet, lässt sich nicht abstrakt bestimmen, sondern hängt von dessen konkretem Aufbau ab. Zu den gefährdeten Systemen zählen nicht nur solche, die personenbezogene Daten verarbeiten; auch vernetzte Industrieroboter, Kraftwerksturbinen oder Pipelines sind typische Angriffsziele.[9] Der System- und Netzwerkschutz steht traditionell im Zentrum des IT-Sicherheitsrechts und bildet nach wie vor den Schwerpunkt der Regelungen im BSIG (vgl. §§ 8a ff. BSIG). Aus regulatorischer Sicht wird hier versucht, Nutzer und Betreiber informationstechnischer Systeme und Netzwerke für die Gewährleistung der Sicherheit „ihrer" Systeme in die Pflicht zu nehmen.[10] Orientierung für die fachliche Umsetzung geben zahlreiche technische Standards und Richtlinien zur sicheren Gestaltung von IT-Systemen und Netzwerken, etwa der IT-Grundschutz-Katalog des BSI für IT-Systeme.[11]

Die *zweite* Ebene ist die Komponentensicherheit: System- und Netzwerkbetreiber sind in ihren Bemühungen um Absicherung der eigenen Systeme ihrerseits auf sichere Software und Hardware angewiesen. Sowohl konkrete Kodierungsfehler als auch die Software- und Hardware-Gestaltung können die Vulnerabilität von IT-Systemen erhöhen. Dass praktisch jede Software Fehler aufweist,[12] heißt nicht zwingend, dass ihre

[7] Die Begriffe „Schwachstelle" („weakness") und „(IT-)Sicherheitslücke" werden weitgehend austauschbar verwendet. Aus technischer Sicht siehe bspw. *IETF*, Internet Security Glossary RFC 2828 (May 2000), https://datatracker.ietf.org/doc/html/rfc2828: „A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy". Das BSIG verwendet den Begriff der Sicherheitslücke, der in § 2 Abs. 6 BSIG wie folgt definiert wird: „Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können." Die NIS 2-RL spricht wiederum von „Schwachstellen" und definiert diese in Art. 6 Nr. 15 NIS 2-RL als eine „Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann".

[8] Zur Produktivität von Schichtenmodellen im Kontext von Untersuchungen zur Technologieregulierung grundlegend *Benkler*, Fed. Comm. L. J. 52 (2000), 561 (562); *Lessig*, Duke L. J. 51 (2002), 1738 (1786); *Solum/Chung*, Notre Dame L. Rev. 79 (2004), 815 (816 ff.).

[9] Zur Gefährdungslage siehe *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, 2022.

[10] Vgl. dazu im Detail *Wischmeyer* (Fn. 6), S. 192 ff. m. w. N.

[11] Vgl. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.

[12] Vgl. zu dieser als „Assume-Breach-Paradigma" bezeichneten Diagnose auch BVerfG, NVwZ 2021, 1361, Rn. 38 m. w. N.

Nutzung gefährlich ist, da nicht alle Fehler sicherheitstechnisch relevant sind.[13] Vielmehr muss es die Schwachstelle Unbefugten gerade ermöglichen, Zugriff auf das die Software verwendende IT-System oder Netzwerk zu erlangen.[14] Ob und inwieweit Schwachstellen ein Risiko für den Systemgebrauch und damit eine Sicherheitslücke begründen, hängt also von ihrer Art, der Qualität des Angriffs und den Sicherheitsmaßnahmen des Systems ab. Jüngere Rechtsakte, etwa der EU Cybersecurity Act (CSA) und der noch im legislativen Verfahren befindliche EU Cyber Resilience Act (CRA), beziehen daher mehr und mehr auch die Hersteller von IT-Komponenten in die Informationssicherheitsregulierung ein und definieren Mindeststandards für die Komponentensicherheit. Die damit verbundenen regulatorischen Probleme sind nicht trivial. So muss etwa berücksichtigt werden, dass die Entwicklung von IT-Komponenten heute regelmäßig ein vielschichtiger, oft hochgradig arbeitsteiliger Prozess ist.[15]

Die *dritte*, bisher am wenigsten verrechtlichte Ebene, betrifft die Internetarchitektur: Bei der Internetsicherheit handelt es sich aus technischer Sicht um einen Sonderfall der Netzwerksicherheit, dessen Regulierung allerdings mit besonderen Herausforderungen konfrontiert ist, weil es – anders als sonst typischerweise bei Netzwerken – an einer einheitlichen Verwaltungsinstanz für das Internet („Netzwerk der Netzwerke") fehlt. Dabei muss berücksichtigt werden, dass die strukturellen Defizite der Internetarchitektur in Sachen Sicherheit nicht nur für die Integrität und Stabilität des Internets selbst eine Bedrohung darstellen, sondern auch für Angriffe auf alle an das Internet angeschlossenen Systeme ausgenutzt werden können.[16]

Diese idealtypische Abschichtung der Problemebenen darf nicht darüber hinwegtäuschen, dass praktische Ansätze zur Verbesserung der IT-Sicherheitslage sowohl aus informations- als auch aus regulierungstechnischer Sicht stets eine integrierte Perspektive erfordern, also mögliche Wechselwirkungen zwischen den verschiedenen Quellen der Unsicherheit berücksichtigen müssen.

---

[13] Eine standardisierte Klassifikation bekannter Schwachstellen bietet das Common Weakness Enumeration System (CWE), abrufbar unter http://cwe.mitre.org/about/index.html. Konkrete Schwachstellen werden klassifiziert nach dem Common Vulnerabilities and Exposures System (CVE), abrufbar unter: https://www.cve.org. Die Schwere von Schwachstellen kann nach dem Common Vulnerability Scoring System bestimmt werden (CVSS), abrufbar unter https://www.first.org/cvss/. Vgl. überblicksartig auch *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), 2020, Kap. 2 Rn. 155 ff.

[14] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, 2020, S. 22 ff.

[15] Vgl. die präzise Beschreibung in ErwGr 11 CSA: Vielfach verwenden Hersteller „von Dritten entwickelte Technologien und Bestandteile wie Software-Module, Bibliotheken oder Programmierschnittstellen [...] und sind von diesen abhängig".

[16] Beispielhaft sei hier auf die Lücken des sog. Border Gateway Protocol (BGP) verwiesen: *Lystrup*, BGP and the System of Trust that Runs the Internet Pt. 1, 21.9.2021, https://umbrella.cisco.com/blog/bgp-and-the-system-of-trust-that-runs-the-internet-pt-1. Zur relativen Blindheit der Internetarchitektur für Sicherheitsbelange instruktiv *DeNardis*, IEEEA 37:2 (2015), 72 ff. Zu grundlegenden Fragen der Gestaltung der Internet-Protokolle siehe *Mueller*, Ruling the Root, 2002; *DeNardis*, Protocol Politics, 2009; *Mueller*, Networks and States, 2010.

II. Zur verfassungsrechtlichen Verantwortung des Staates im Umgang mit den Risiken der digitalen Technik

Auf die überaus komplexen technischen Herausforderungen reagieren Staaten weltweit mit immer dichteren politischen und auch rechtlichen Vorgaben.[17] Die entsprechenden Regelungen sind auf eine Vielzahl von Rechtsakten verteilt, vom Datenschutzrecht über das Recht kritischer Infrastrukturen bis hin zum Energiewirtschaftsrecht. In Deutschland finden sich die maßgeblichen Regelungen vor allem im BSIG, das sich durch die letzte Novelle vom 28.5.2021 (IT-SiG 2.0[18]) mehr und mehr als „Querschnittsgesetz" für die IT-Sicherheit profiliert hat. Eine ähnliche Funktion hat in Europa die NIS 2-Richtlinie.[19] Der Unionsgesetzgeber hat daneben zahlreiche weitere Gesetze verabschiedet; verschiedene Vorhaben sind zudem aktuell in der Planung oder bereits im Gesetzgebungsverfahren.[20] In Deutschland liegt für die bis Oktober 2024 geschuldete Umsetzung der NIS 2-Richtlinie der Referentenentwurf für ein „NIS 2 Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG) vor, das unter anderem zu einer erheblichen Ausweitung des Adressatenkreises des Informationssicherheitsrechts führen wird.[21] Hier ist eine Rechtsmaterie in Entstehung begriffen, deren Umfang und Bedeutung die Rechtswissenschaft gerade erst zu realisieren beginnt.

Diese Gesetzgebung ist nun nicht nur – das ist hier der entscheidende Punkt – ein Produkt politischer Opportunität. Vielmehr kommt der Staat mit der Förderung der (Informations-)Sicherheit seiner verfassungsrechtlichen Verantwortung zur Sicherheitsgewährleistung für die digitale Gesellschaft nach. Eine solche Verantwortung des Staates für die Risiken der Technik gehört seit geraumer Zeit zum gesicherten Bestand

[17] Vgl. die Länderberichte unter https://css.ethz.ch/en/publications/risk-and-resilience-reports. Die Schriftenreihe „SpringerBriefs in Cybersecurity" bündelt gleichfalls eine größere Zahl länderspezifischer Darstellungen.

[18] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18.5.2021, BGBl. I S. 1122. Vgl. zu den Regelungsinhalten im Überblick *Hornung*, NJW 2021, 1985. Zum Gesetz ausführlich auch *Schallbruch*, CR 2021, 450; *ders.*, CR 2021, 516; sowie die Dokumentation und den Kommentar von Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022.

[19] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, ABl. L 333/80.

[20] Programmatisch: *Europäische Kommission/Hoher Vertreter der Union für Außen- und Sicherheitspolitik*, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final. Aus der Literatur zur Unionalisierung des Cybersicherheitsrechts: *Calliess/Baumgarten*, German L. J. 21 (2020), 1149; *Bendiek/Maat*, The EU's Cybersecurity Policy, in: Siboni/Ezioni (Hrsg.), Cybersecurity and Legal-Regulatory Aspects, 2021, S. 23 ff.; *Wischmeyer* (Fn. 6), S. 274 ff.

[21] Vgl. die Dokumentation des Diskussionsstandes unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

der Verfassungsdogmatik; sie wurde zunächst für das Umwelt-, Technik- und Atomrecht entwickelt und muss heute für den Themenkreis Informationssicherheit aktualisiert werden.[22]

Verfassungsrechtlich ist diese Verantwortung in erster Linie in den Grundrechten verankert. Dort begegnet sie im Falle der IT-Sicherheit primär in der Verpflichtung des Staates (unverhältnismäßige) Eingriffe in die IT-Sicherheit zu unterlassen. Je mehr Lebensbereiche und damit verbundene Grundrechtsfunktionen von der Vertraulichkeit, Verfügbarkeit und Integrität der dafür genutzten informationstechnischen Systeme abhängen, desto weiter reicht der auf diese Weise zu gewährende Schutzanspruch. Standen in der Vergangenheit zunächst Angriffe auf die Vertraulichkeit von IT-Systemen und damit auf den grundrechtlichen Privatheitsschutz im Vordergrund – bereits 2007 war das Instrument der Online-Durchsuchung Anlass für das BVerfG, sich insoweit mit der grundrechtlichen Dimension der IT-Sicherheit zu befassen[23] –, greift das Problem der IT-Sicherheit heute viel weiter aus. So können die geschützten Belange „so mannigfaltig sein wie der weite Kreis aller IT-gestützten gesellschaftlichen oder privaten Vorgänge und Abläufe selbst".[24] Unter den gegenwärtigen Bedingungen kann sichere und funktionierende Informationstechnik somit durchaus auch als allgemeine Wirksamkeitsvoraussetzung der Grundrechte verstanden werden. Die vom BVerfG 2007 aus dem allgemeinen Persönlichkeitsrecht und dem Schutz der Privatheit hergeleitete Pflicht des Staates, die Vertraulichkeit und Integrität informationstechnischer Systeme vor Angriffen Dritter zu schützen – das sogenannte „IT-Grundrecht" – ist daher in diesem umfassenden Sinne fortzuentwickeln.

Die Grundrechte beschränken allerdings nicht nur staatliches Handeln, das die IT-Sicherheit kompromittiert. Insbesondere dann, wenn Gefährdungen durch private Dritte oder auch durch Drittstaaten drohen, folgt aus der objektiv-rechtlichen Funktion aller davon konkret betroffener Grundrechte die Verpflichtung des Staates, Verfahren zur Hebung des Sicherheitsniveaus oder zu sonstigen Schutzvorkehrungen zu

[22] Grundlegend BVerfGE 53, 30 (57 f.). Aus der Literatur nach wie vor maßgeblich *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985; sowie die Referate zum Oberthema „Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht" von *Ipsen*, in: VVDStRL 48 (1990), S. 187 ff.; *Murswiek*, in: VVDStRL 48 (1990), S. 207 ff.; *Schlink*, in: VVDStRL 48 (1990), S. 235 ff.

[23] BVerfGE 120, 274. Dazu erläuternd *Hoffmann-Riem*, JZ 63 (2008), 1009 (1014, 1022). Konstruktiv-kritisch dazu *Britz*, DÖV 2008, 411; *Eifert,* NVwZ 2008, 521.

[24] *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 37, die fortfahren: „Wo IT-Systeme etwa Beatmungsmaschinen in Krankenhäusern steuern, ist das Recht auf Leben und körperliche Unversehrtheit betroffen (Art. 2 Abs. 2 S. 1 GG); wo politische Demonstrationen über Messaging-Dienste oä koordiniert werden, kann es auch unabhängig von der Erfassung personenbezogener Daten – etwa bei einem rein physischen Einwirken auf die Server – um das Recht auf Versammlungsfreiheit (Art. 8 GG) gehen, usw."

ergreifen, um auf diese Weise die Betroffenen zu schützen.[25] Welche Folgerungen dies konkret sind, lässt sich nur für den jeweiligen Einzelfall auf Grundlage einer Analyse der einschlägigen Grundrechtsnormen und der konkreten Gefährdungssituation entwickeln. Denn eine allgemeine Pflicht zur Gewährleistung *der* Informationssicherheit existiert ebenso wenig wie eine allgemeine Pflicht zur Gewährleistung *der* technischen Sicherheit oder sonstiger Sicherheiten. Der Gesetzgeber, der seiner verfassungsrechtlichen Verantwortung gerecht werden will, muss sich also stets sachbereichsbezogen der jeweils drängendsten IT-Sicherheitsproblemlagen vergegenwärtigen und entsprechend aktiv werden. Dem dienen in erster Linie die gerade beschriebenen gesetzgeberischen Initiativen zur Schaffung eines robusten Informationssicherheitsrechts. Diese Verantwortung beeinflusst aber auch – und hierauf konzentrieren sich die folgenden Ausführungen –, wie der Staat selbst mit Sicherheitslücken hantieren kann.

C. Risiken der staatlichen Nutzung von IT-Sicherheitslücken und ihre verfassungsrechtliche Verarbeitung

Staatliche Stellen können IT-Sicherheitslücken potenziell für alle möglichen strategischen Ziele, für die der Zugriff auf IT-Systeme Dritter entscheidend ist, nutzen. In der Praxis dominieren bisher vor allem nachrichtendienstliche und sonstige ermittlungsbehördliche, also auf Informationsabschöpfung konzentrierte Ziele wie im Fall Pegasus. Insbesondere im Fall zwischenstaatlicher Konflikte werden jedoch auch wesentlich weiterreichende Interventionen diskutiert oder international bereits praktiziert. Ungeachtet der Vielzahl möglicher Einsatzkontexte und -motive eint die Maßnahmen auf technischer Ebene, dass staatliche Stellen mit IT-Schwachstellen operieren müssen, um in die Zielsysteme eindringen und dort ihre Späh- oder sonstigen Schadprogramme einbringen zu können.[26] Das staatliche Know-how wird hier also nicht dafür eingesetzt, erkannte Schwachstellen zu beherrschen und zu beseitigen. Vielmehr verschafft sich der Staat Kenntnis von Schwachstellen, sieht dann jedoch – abweichend von den Grundregeln des allgemeinen IT-Sicherheitsrechts[27] – von deren Veröffentlichung ab. Solche Maßnahmen gefährden potenziell alle möglichen Rechtsgüter, in erster Linie die individuelle Privatsphäre. Sie begründen darüber hinaus aber auch spezifische Risiken für die IT-Sicherheit. Diese über die eigentliche Maßnahme hinausgehenden Risiken sollen nun zunächst beschrieben werden (I.). Anschließend ist am Beispiel der sogenannten

[25] Ansätze in diese Richtung enthält die vom BVerfG betonte (auch) objektiv-rechtliche Dimension des IT-Grundrechts: BVerfGE 120, 274 (306); BVerfG, NVwZ 2021, 1361, Rn. 33. Ob weitere verfassungs-, aber nicht spezifisch grundrechtlich radizierte Verpflichtungen staatlicher Stellen, das Informationssicherheitsniveau zu heben, existieren, muss hier ausgeklammert werden, vgl. bspw. *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 211.

[26] Die folgenden Absätze orientieren sich eng an *Wischmeyer* (Fn. 6), S. 281 ff.

[27] Dazu *Wischmeyer* (Fn. 6), S. 217 ff., 226 ff.

Quellen-TKÜ – aktuell wohl die „Standardmaßnahme“ für Eingriffe in die IT-Sicherheit durch deutsche Behörden – zu fragen, ob unsere Rechtsordnung diese Risiken bereits angemessen verarbeitet (II.).

I. Implikationen der Nicht-Offenlegung und Nutzung von Schwachstellen für die IT-Sicherheit: Kollisions-, Proliferations- und Einsatzrisiken

Wenn staatliche Stellen Kenntnisse über informationssicherheitsrelevante Schwachstellen von Programmen, Systemen, Netzwerken etc. nutzen, erzeugt dies drei Arten IT-sicherheitsspezifischer Risiken:

Zunächst ist es oft nicht möglich, sicher auszuschließen, dass Schwachstellen, die von staatlichen Stellen gefunden oder erworben wurden, bereits Dritten bekannt sind und von diesen ausgenutzt werden. Immer wenn der Staat Schwachstellen, von denen er Kenntnis erlangt hat, nicht veröffentlicht, muss er daher damit rechnen, dass auch diesen Dritten die ungestörte Nutzung möglich bleibt.[28] Dieses hier sogenannte *Kollisionsrisiko* ist besonders hoch, wenn staatliche Stellen von den Lücken nicht durch eigene Forschung, sondern durch ausländische Partnerdienste Kenntnis erlangt haben oder die Lücken auf schwarzen oder grauen Märkten erworben haben.[29] In solchen Fällen ist offensichtlich, dass alle möglichen staatlichen und nicht-staatlichen Akteure die Lücke nutzen. Wenn sich der Staat in dieser Situation gegen eine Offenlegung entscheidet, akzeptiert er stets die mögliche Beeinträchtigung seiner Bürger durch beliebige Dritte.

Selbst dann, wenn staatliche Stellen exklusiv Kenntnis von einer Schwachstelle haben sollten, begründet die Nichtoffenlegung dieser Information IT-sicherheitsspezifische Risiken. Dies liegt daran, dass die Behörde selbst Opfer von Cyberangriffen werden kann oder die Information anderweitig unbefugt verbreitet werden können, etwa durch Leaks. Dieses *Proliferationsrisiko* ist der Öffentlichkeit insbesondere durch den Angriff der sogenannten „Shadow Brokers“-Gruppe auf die U.S. National Security Agency (NSA) vor Augen geführt worden, bei dem zahlreiche hochpotente Schwachstellen aus dem NSA-Arsenal gestohlen wurden und sich alsbald in zahlreichen hochpotenten Angriffsinstrumenten fanden.[30] Durch die Vorhaltung von Schwachstellen

[28] Vgl. zu diesem Phänomen nur *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 29 f. m. w. N., https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.

[29] Zu den Märkten für Software-Schwachstellen näher *Meakins*, Journal of Cyber Policy 4:1 (2019), 60; *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, S. 14 ff. m. w. N., https://www.swp-berlin.org/publikation/governance-von-0-day-schwachstellen.

[30] Vgl. zu den „Verlusten“ der NSA durch die Angriffe der sog. „Shadow Brokers“-Gruppe die Darstellung unter https://en.wikipedia.org/wiki/The_Shadow_Brokers. Siehe auch die Reportage von *Nakashima/Timberg*, NSA officials worried about the day its potent hacking tool would get loose,

generiert der Staat somit stets aktiv ein gewisses IT-Sicherheitsrisiko, das sich – je nach Verbreitung der betroffenen Schwachstelle – bei einer Vielzahl von Akteuren in Wirtschaft und Gesellschaft realisieren kann. Für die Hersteller der betroffenen Komponenten sowie für die Betreiber von Systemen und Netzwerken, die aufgrund mangelnden Wissens die Schwachstellen nicht beseitigen können, erhöht sich damit zugleich das Risiko von Sanktionen und Haftung – zumal parallele Entdeckungen der Sicherheitslücke durch Dritte ja immer möglich sind. Darüber hinaus sind auch jene staatlichen Akteure gefährdet, die keinen privilegierten Zugang zu diesem Wissen haben und daher nicht proaktiv zur Minderung dieser Risiken handeln können.

Neben der Vorhaltung schafft auch der Einsatz von IT-Schwachstellen, beispielsweise in Form der Quellen-TKÜ, ein weiteres IT-Sicherheitsrisiko: Denn die von staatlichen Stellen verwendeten Schwachstellen könnten Manipulationen an den Ziel-Systemen ermöglichen, die über den beabsichtigten oder gesetzlich zulässigen Rahmen der eigentlich intendierten Maßnahme, etwa die Abschöpfung der laufenden Kommunikation, weit hinausgehen. Die staatliche Technik kann dann mehr als das, was die Behörde dürfte. Dieses *Einsatzrisiko* ist eng mit dem üblicherweise nicht IT-sicherheitsspezifischen Zweck der Maßnahme, wie beispielsweise der Beeinträchtigung der Privatsphäre, verbunden; sein normatives Eigengewicht muss jedoch separat gewürdigt werden. Auf diese Thematik wird zurückzukommen sein.

Das hier beschriebene Risikoprofil gilt in erster Linie für sogenannte Zero-Day-Schwachstellen, das heißt, Schwachstellen, die den Herstellern und der Öffentlichkeit unbekannt sind, so dass typischerweise keine Abwehrmaßnahmen, etwa in Form von Updates, zur Verfügung stehen.[31] Die überwiegende Zahl der Angriffe auf IT-Systeme nutzt allerdings Schwachstellen, die bereits bekannt sind („N-Day-Schwachstellen“).[32] Hierbei wird ausgenutzt, dass eine Vielzahl von IT-Systemen und Diensten trotz allgemeiner Kenntnis der Sicherheitslücke für diese anfällig bleibt. Die Gründe hierfür sind vielfältig: So kann es sein, dass die technische Anpassung viel Zeit in Anspruch nimmt, dass die ursprünglich für das Produkt verantwortlichen Stellen den Service bereits eingestellt haben, dass die verfügbaren Patches nicht verwendet werden usw. In jedem Fall sind N-Day-Schwachstellen auch für staatliche Akteure eine attraktive Ressource.

Die Struktur der durch die Nutzung von N-Day-Schwachstellen erzeugten Risiken unterscheidet sich allerdings teilweise von jener, die bei Zero-Day-Schwachstellen entsteht: Das *Kollisionsrisiko* von Zero-Day-Schwachstellen hat sich hier zwar bereits manifestiert, bleibt aber dennoch in begrenztem Umfang bestehen, sofern man davon aus-

---

Washington Post, 16.5.2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

[31] Zum Begriff näher *Schulze* (Fn. 29), S. 7. Vgl. auch *Ablon/Bogart*, Zero Days, Thousands of Nights, 2017.

[32] Hierzu ausführlich *Schulze* (Fn. 29), S. 20.

geht, dass staatliche Aktivitäten zur Schließung der Sicherheitslücke (statt eigener aktiver Nutzung der Lücke), Betroffene dazu motivieren könnte, ihre Maßnahmen zur Abhilfe zu intensivieren. Das *Proliferationsrisiko* ist ebenfalls deutlich verringert. Sofern sich die Schwachstelle durch einen Angriff auf staatliche Stellen allerdings mit geringeren Kosten verschaffen lässt, als dafür auf dem freien Markt bezahlt werden müsste, liegt es allerdings weiterhin über Null. Hinsichtlich des *Einsatzrisikos* bestehen keine signifikanten Unterschiede. Vor allem letzteres löst daher auch für N-Day-Schwachstellen gesetzgeberischen Handlungsbedarf aus; bei der konkreten Ausgestaltung des Schwachstellenmanagements müssen die unterschiedlichen Risikostrukturen von Zero- und N-Day-Schwachstellen allerdings Berücksichtigung finden (dazu unter D.).

II. Zur verfassungsrechtlichen Verarbeitung dieser Risiken am Beispiel der Quellen-TKÜ

Wie verarbeitet unsere Rechtsordnung derzeit diese Risiken? Dieser Frage soll hier durch eine Analyse der verfassungsgerichtlichen Entscheidungen zur Quellen-TKÜ nachgegangen werden.[33]

1. Grundrechtliche Risiken der Quellen-TKÜ

Mit den bundes- und landesrechtlichen Befugnisnormen zur Durchführung einer „Quellen-TKÜ“[34] hat der Sicherheitsgesetzgeber auf die Sorge der Behörden reagiert, durch die zunehmende Verlagerung individueller Kommunikation ins Digitale von bisher zugänglichen Informationsquellen abgeschnitten zu werden („going dark“).[35] Denn die digitale Kommunikation erleichtert den Einsatz von Ende-zu-Ende-Verschlüsselung, die mittlerweile von vielen Kommunikationsanbietern standardmäßig

[33] Nicht näher wird hier auf die sog. Online-Durchsuchung eingegangen. Aus IT-Sicherheitsperspektive unterscheiden sich Quellen-TKÜ und Online-Durchsuchung nur geringfügig, muss doch auch erstere die Daten auf den IT-Systemen der Betroffenen vor deren Verschlüsselung, also vor Einleiten des konkreten Übertragungsvorgangs, bzw. nach Abschluss der Kommunikation, also nach der Entschlüsselung, abgreifen können, wozu typischerweise ein weitreichender Zugriff auf das IT-System selbst erforderlich ist. Dazu aus technischer Sicht näher Hauser, Das IT-Grundrecht, 2015, S. 32 ff.; Freiling/Safferling/Rückert, JR 2018, 9 (16 ff.); Schlegel, Normative Grenzen für internetbasierte Ermittlungsmethoden, 2019, S. 99 ff. Die folgenden Ausführungen orientieren sich erneut eng an Wischmeyer (Fn. 6), S. 285 ff.

[34] Aus dem Bundesrecht vgl. § 100a Abs. 1 Satz 2 und 3 StPO; § 51 Abs. 2 BKAG; § 11 Abs. 1a G 10; § 72 Abs. 3 ZfdG. Aus dem Landesrecht siehe nur beispielhaft Art. 42 Abs. 2 S. 1 BayPAG; § 54 Abs. 2 PolG BW; § 15b HSOG.

[35] Diskursprägend hierzu die mit „Going Dark: Lawful Electronic Surveillance in the Face of New Technologies“ betitelte Anhörung eines Unterausschusses des Committee on the Judiciary des U.S.-Repräsentantenhauses am 17.2.2011, dokumentiert unter https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/pdf/CHRG-112hhrg64581.pdf. Zur Debatte aus deutscher Sicht, primär aus Sicht der deutschen Sicherheitsbehörden, siehe die Beiträge im Band von Lindner/Unterreitmeier (Hrsg.), Going dark – Signals Intelligence im IT-Zeitalter, 2023.

angeboten wird. Bei Ende-zu-Ende-Verschlüsselung laufen die herkömmlich beim Telekommunikationsmittler ansetzenden Überwachungsmethoden (vgl. §§ 170 f. TKG) bekanntlich ins Leere. Um dem entgegenzuwirken, sollen die Behörden daher nun direkt auf den beteiligten Endgeräten Software installieren dürfen, mit deren Hilfe die Telekommunikation bereits an der „Quelle" bzw. an der „Mündung" abgeschöpft werden kann. Hierzu werden in aller Regel Schwachstellen der Zielsysteme oder sonstige Sicherheitslücken ausgenutzt. Das BVerfG hat das hierzu in tatsächlicher Hinsicht erforderliche Vorgehen in einem Senatsbeschluss von 2021 („IT-Sicherheitslücken-Beschluss") wie folgt erläutert: „Die Ausnutzung von Sicherheitslücken [...] ist eine von mehreren Möglichkeiten, wie eine Quellen-TKÜ [...] durchgeführt werden kann. Zur Ermöglichung einer solchen Überwachung muss das Zielsystem mit einer Überwachungssoftware infiltriert werden. Auf welche Weise dies geschieht, ist gesetzlich nicht geregelt. Denkbar ist eine Infiltration auf physischem Weg. Dabei wird die Software durch einen Ermittler vor Ort auf das Zielsystem aufgespielt, etwa nach einem heimlichen Betreten der Wohnung, [...]. Alternativ kann das Zielsystem über einen Fernzugriff infiltriert werden. Dies kann geschehen, indem der Zielperson die Infiltrationssoftware als E-Mail-Anhang zugespielt und dann von dieser Person geöffnet wird oder indem Sicherheitslücken in der Hard- oder Software des Zielsystems ausgenutzt werden. Letzteres kann insbesondere im Vergleich zu den sich aus Art. 13 GG ergebenden Grenzen für ein physisches Betreten der Wohnung und zu Zugriffen, die ein Fehlverhalten des Nutzers voraussetzen, praktische Vorteile bieten."[36]

Über die verfassungsrechtliche Zulässigkeit dieser Maßnahme wird bereits seit geraumer Zeit gestritten.[37] Auch das BVerfG hat bereits mehrfach zu entsprechenden Ermächtigungsgrundlagen Stellung genommen.[38] Dabei hat sich die bisherige Befassung jedoch ganz auf Umfang und Grenzen der Verarbeitung der mittels solcher Eingriffe gewonnenen persönlichen Daten konzentriert. Stark umstritten ist etwa, ob der Gesetzgeber den behördlichen Zugriff auf solche Daten im Zielsystem erweitern darf, die dort auch nach Abschluss des Telekommunikationsvorgangs gespeichert bleiben.[39] Auch

[36] BVerfG, 1 BvR 2771/18 v. 8.6.2021, Rn. 5 (insoweit nicht abgedruckt in NVwZ 2021, 1361).

[37] Vgl. beispielhaft *Roggan*, StV 2017, 821; *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 62 ff.; *Martini/Fröhlingsdorf*, NVwZ-Extra 24 2020, 1.

[38] Hierzu BVerfGE 120, 274 (309, Rn. 190); 141, 220 (309, Rn. 228). Gegen § 100a Abs. 1 S. 2 StPO in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.8.2017 (BGBl. I S. 3202) wurden verschiedene Verfassungsbeschwerden eingelegt. Mit Beschluss der 2. Kammer des Ersten Senats vom 17.4.2023 (1 BvR 176/23 und 1 BvR 178/23) wurden die für den Aspekt IT-Sicherheit besonders relevanten Verfassungsbeschwerden nunmehr für unzulässig erklärt, vgl. dazu die Stellungnahme der Beschwerdeführer: *Bundesverbund IT-Sicherheit e.V. (Teletrust)*, Stellungnahme, 17.7.2023, https://www.teletrust.de/fileadmin/user_upload/230717-TeleTrusT-Kommentierung_Abweisung_Verfassungsbeschwerde.pdf.

[39] Dies dürfte auszuschließen sein. Hochproblematisch ist daher § 100a Abs. 5 Nr. 1b StPO, der aufgrund der oft längeren Frist, die zwischen rechtlicher Anordnung der Maßnahme und faktischem Zugriff liegt, die Erhebung aller Daten ab Anordnung der Maßnahme ermöglicht.

der Schutz des Kernbereichs ist ein zentrales Thema. Weniger Beachtung hat demgegenüber gefunden, dass die Quellen-TKÜ aus technischer Sicht kein Äquivalent zur hergebrachten TKÜ ist. Letztere erzeugt insbesondere keine bzw. ganz anders gelagerte und weniger weitreichende Einsatz-, Kollisions- und Proliferationsrisiken.

2. Unzureichende Würdigung des Einsatzrisikos

Diese IT-spezifische Risikodimension der Quellen-TKÜ wird in der Rechtsprechung des BVerfG bisher allerdings nicht hinreichend adressiert. Dies gilt zunächst für das Einsatzrisiko. Dass das Gericht der mit der Nutzung von IT-Sicherheitslücken notwendig verbundenen Beeinträchtigung der IT-Sicherheit kein über den Eingriff in die kommunikative Privatheit hinausgehendes Eigengewicht zuspricht, zeigt sich bereits daran, dass es den Einsatz der Quellen-TKÜ nur auf seine Vereinbarkeit mit Art. 10 GG und nicht auch mit dem IT-Grundrecht prüfen will.[40] Dementsprechend gerät auch das mit der Quellen-TKÜ verbundene Risiko einer „überschießenden" Überwachung nicht richtig in den Blick. Dieses Einsatzrisiko ist insbesondere dann hoch, wenn die handelnde Behörde die Funktionalitäten der Software nicht umfassend nachvollziehen und Fehl- oder Fremdnutzungen des Einsatzes, etwa durch die damit beauftragten Dienstleister, nicht sicher ausschließen kann.[41] Die gesetzlichen Befugnisnormen sehen weder besondere Sicherungsmechanismen vor noch verlangen sie eine bestimmte, solchen Missbrauch ausschließende Technikgestaltung. Wie in das Zielsystem eingedrungen wird, wird meist nur ganz generisch in der Form beschrieben, dass „mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen [werden darf], wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen" (§ 100a Abs. 1 S. 2 StPO). Das BVerfG betont zwar, dass die Quellen-TKÜ auf laufende Telekommunikationsvorgänge beschränkt bleiben *muss*. Ob und wie dies technisch gesichert werden kann, will das Gericht jedoch nicht prüfen; dies betreffe nur „die Anwendung der Norm, nicht aber ihre Gültigkeit."[42] Dies verkennt, dass die Einbringung von Quellen-TKÜ-Software in das Zielsystem keineswegs ein minimalinvasiver Eingriff ist; dieses wird vielmehr grundlegend kompromittiert.[43] Dementsprechend sind komplexe technische Mittel (Filter) erforderlich, um „nur" die laufende Kommunikation abzuschöpfen. Vor

[40] Vgl. BVerfGE 141, 220 (311, Rn. 234). Kritisch *Martini*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 10 Rn. 196 f.; *Wischmeyer*, in: Dreier, GG, Bd. I, 4. Aufl., 2023, Art. 10 Rn. 125. Eine gewisse Öffnung ist erkennbar in BVerfG, NVwZ 2021, 1361, Rn. 29.

[41] Vgl. den entsprechenden Parteivortrag bei BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 7.

[42] Vgl. BVerfGE 141, 220 (311, Rn. 234).

[43] Siehe hierzu die instruktive Aufbereitung des „Telegram"-Falls bei *Herpig*, Government Hacking, Juni 2017, S. 7 ff., https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf.

diesem Hintergrund erscheint es sowohl unter Bestimmtheits- als auch unter Verhältnismäßigkeitsgesichtspunkten zwingend, dass auch die Geltung einer Befugnisnorm in Frage steht, wenn diese gar keine Vorgaben zu technischen und organisatorischen Sicherungsmechanismen enthält, mit deren Hilfe die Behörden die Risiken der von ihnen eingesetzten Technik überschauen und beherrschen können.

In einem weiteren Beschluss von 2022 hat das BVerfG dieses Problem durchaus zur Kenntnis genommen. Es hat aber im Ergebnis genügen lassen, dass das Bundeskriminalamt zur Einhegung des Einsatzrisikos einen „Gesamtabnahmeprozess" vorsieht.[44] Allerdings muss bezweifelt werden, dass dieser Prozess einen hinreichenden Sicherungsmechanismus etabliert. Offen ist bereits, welche rechtliche Bindungswirkung dieser in Form eines auf der Homepage des Bundeskriminalamts veröffentlichten Schreibens dokumentierte Abnahmeprozess überhaupt erzeugt. Auch inhaltlich enthält das referenzierte Dokument nur wenige belastbare Ausführungen und misst zudem an entscheidenden Punkten den Eigenerklärungen der externen Dienstleister ein hohes Gewicht bei. Angesichts des erheblichen Kompetenzgefälles zwischen staatlichen Behörden und privaten Dienstleistern sowie der spezifischen Marktdynamiken im Bereich IT-basierter Überwachungsdienstleistungen erscheint das Vertrauen des BVerfG auf die grundrechtssichernde Funktion des Gesamtabnahmeprozesses daher nicht gerechtfertigt. Insgesamt hat das BVerfG die IT-sicherheitsbezogenen Einsatzrisiken der Quellen-TKÜ somit bisher nur unvollständig erfasst.[45]

3. Unzureichende Würdigung der Kollisions- und Proliferationsrisiken

Gleiches gilt für die durch die Quellen-TKÜ erzeugten Kollisions- und Proliferationsrisiken. Auf diese hatten die Beschwerdeführer in der Gesetzesverfassungsbeschwerde, die dem Beschluss vom Juni 2021 zu Grunde lag, das BVerfG explizit aufmerksam gemacht. So hatten sie ihre Behauptung einer Verletzung der aus dem IT-Grundrecht rührenden Schutzpflicht damit begründet, dass die Norm einen Anreiz für Behörden und IT-Sicherheitsforschende setze, entdeckte Schwachstellen nicht den jeweiligen Herstellern bzw. Betreibern zu melden, sondern für eigene Zwecke zu nutzen bzw. an die Behörden zu veräußern. Notwendig sei daher mit Blick auf den Vorbehalt des Gesetzes eine formell-gesetzliche Grundlage für die Nicht-Veröffentlichung, die zudem organisatorische und prozedurale Mindeststandards für den Erwerb und den weiteren

[44] Vgl. BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 19. Gemeint ist wohl *BKA*, Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen- Telekommunikationsüberwachung und der Online- Durchsuchung, 5.10.2018, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.html.

[45] Keine intensivere Prüfung erfolgt in BVerfGE 162, 1 Rn. 111; BVerfG, 1 BvR 176/23 v. 17.4.2023, Rn. 5 f.

Umgang mit Schwachstellen sowie zum Schutz vor einer Proliferation der Schwachstellen an nicht autorisierte Dritte enthalte.[46] Angegriffen wurde also die nur auf den ersten Blick „technikneutrale" Regelungskonzeption des Gesetzgebers, die sich bei genauerer Betrachtung als Delegation grundrechtlich sensibler Entscheidungen an die Exekutive erweist. Denn ebenso wie die sonstigen, weitgehend analog strukturierten Ermächtigungen zur Quellen-TKÜ im Bundes- und im Landesrecht beschränkte die angegriffene Norm die Exekutive in keiner Weise darin, sich in großem Umfang hochpotente Sicherheitslücken zu verschaffen und diese zu bevorraten; auch für die Sicherung vor Verlust und gegen eine (unbefugte) Weitergabe werden weder hier noch an anderer Stelle spezifische Vorkehrungen verlangt.

Das BVerfG hat diese Argumentation zwar zur Kenntnis genommen. Es hat zudem ausdrücklich anerkannt, dass die Pflicht des Staates zum Schutz der IT-Sicherheit eine „Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits" verlange.[47] Aus dieser zutreffenden Rekonstruktion der Ausgangslage hat das Gericht dann jedoch keine hinreichenden Schlüsse gezogen.

So hat das BVerfG schon nicht näher erörtert, wie die Entscheidung über die Nichtveröffentlichung und Bevorratung von Schwachstellen, die einer Nutzung von Zero- und (typischerweise) N-Day-Exploits in Form der Quellen-TKÜ vorausgeht, grundrechtsdogmatisch einzuordnen ist. Zwar erleichtert das Unterlassen einer Veröffentlichung in erster Linie privaten Dritten Angriffe auf die IT-Sicherheit, was eine Schutzpflichtkonstellation nahelegt. Erhält der Staat allerdings durch Dritte Kenntnis von der Sicherheitslücke, muss er damit rechnen, dass nicht er allein, sondern auch weitere Akteure diese ausnutzen. Unter diesen Umständen kommt die Entscheidung zur eigenen Nutzung, der keine entsprechenden Aktivitäten zur Schließung der Lücke korrespondieren, einer aktiven Billigung des Risikos gleich, das mit der Qualifikation als Unterlassen einer eigenen Eingriffshandlung und der daran anknüpfenden Einstufung als Frage der grundrechtlichen Schutzpflicht kaum mehr adäquat beschrieben erscheint. Zwar dürfte nach hergebrachter Dogmatik auch die Schwelle zum eigenen „aktiven" Eingriff nicht überschritten sein. Dass sich eine Schutzpflichtkonstellation jedoch immer mehr zu einem konkreten Handlungsgebot verengen kann, je dichter die fragliche Maßnahme in den Kontext staatlichen Eingriffshandelns eingebunden ist, ist kein der verfassungsrechtlichen Dogmatik fremder Gedanke. So hat das BVerfG im Kontext der

[46] BVerfG, 1 BvR 2771/18 v. 8.6.2021, Rn. 10 (insoweit nicht abgedruckt in NVwZ 2021, 1361).

[47] BVerfG, NVwZ 2021, 1361, LS 2b. Zurückhaltender nun BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 17: „Zwar kann [...] sich hieraus eine konkrete Schutzpflicht des Gesetzgebers ergeben, den Umgang mit Sicherheitslücken zu regeln".

in ähnlicher Form zwischen Abwehrrecht und Schutzpflicht changierenden Vorratsdatenspeicherung mit Blick auf die Gefahren eines illegalen Zugriffs auf die bei den Privaten anfallenden Vorratsdaten verlangt, dass für die im Zusammenhang mit dem staatlichen Ermittlungsinteresse bevorrateten Daten „ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht", gewährleistet wird.[48] Auch wenn das Grundgesetz „nicht detailgenau" vorgebe, welche Sicherheitsmaßnahmen im Einzelnen geboten seien, unterliege dies einer verfassungsgerichtlichen Nachprüfung; der üblicherweise bei Schutzpflichten bestehende Gestaltungsspielraum wurde vom Gericht hier wesentlich verengt.[49]

Diesen Weg ist das BVerfG im IT-Sicherheitslücken-Beschluss und in den Folgeentscheidungen zum Bayerischen Verfassungsschutzgesetz und zu § 100a Abs. 1 Satz 2 und 3 StPO nicht gegangen. Stattdessen hat das BVerfG die Frage ohne Diskussion als Schutzpflichtproblematik eingeordnet. Damit ließ sich das Vorbringen der Beschwerdeführer aber schnell und umfassend abtun. Denn die Zulässigkeitsanforderungen bei Gesetzesverfassungsbeschwerden sind in Schutzpflichtkonstellationen aus prozessualen Gründen – zu Recht – sehr hoch.[50] Dass die Beschwerdeführer den Anforderungen an die Darlegungslast für die Verletzung einer staatlichen Schutzpflicht nicht genügt hatten, ließ sich dementsprechend leicht begründen.[51] Zur Sache hat das Gericht daher gar nicht Stellung genommen.

4. Folgerungen aus der Verfassungsrechtsprechung

Die Frage, wie sich die durch die staatliche Nutzung von IT-Sicherheitslücken entstehenden Einsatz-, Kollisions- und Proliferationsrisiken für die Grundrechte einhegen lassen, besteht letztlich unabhängig von der demokratie- und gewaltenteilungstheoretisch fundierten Frage, inwieweit gerade das BVerfG dazu berufen ist, den Gesetzgeber an seine diesbezüglichen Handlungspflichten zu erinnern. Die Tatsache, dass sich das Gericht hier nicht zu einer expliziten Stellungnahme für eine Regulierungspflicht ausgesprochen hat, heißt daher nicht, dass nicht gewichtige grundrechtliche Belange dafür streiten, die genannten Risiken endlich legislativ einzuhegen. Eben hierfür bedarf es eines staatlichen Schwachstellenmanagements.

---

[48] BVerfGE 125, 260 (325, Rn. 222).

[49] BVerfGE 125, 260 (326, Rn. 224).

[50] *Buchheim*, Die Grenzen des „entgrenzten Gerichts", VerfBlog, 27.7.2021, https://verfassungsblog.de/die-grenzen-des-entgrenzten-gerichts/, unter Verweis auf *Möllers*, Funktionen des Verfassungsprozessrechts, in: Münch/Thiele (Hrsg.), GS Heun, 2019, S. 149 ff.

[51] BVerfG, NVwZ 2021, 1361, Rn. 48 ff. Entsprechend BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 16 ff. Inwieweit die vom BVerfG in der Entscheidung konkret vorgebrachten Gründe überzeugen können, sei hier dahingestellt. Kritisch dazu *Wischmeyer* (Fn. 6), S. 289 ff.

D. Grundzüge eines staatlichen Schwachstellenmanagements

I. Ziele und Orientierungspunkte

Auch die Politik hat die grundrechtliche Relevanz dieses Instruments mittlerweile erkannt: So sieht der Koalitionsvertrag die Einführung eines wirksamen Schwachstellenmanagements vor und das Bundesministerium des Innern führt das Projekt auf seiner Liste der „Zentralen Vorhaben" für 2023.[52] Allerdings lässt die praktische Umsetzung derzeit noch auf sich warten. Welche Ursachen regierungsintern für die Verzögerung verantwortlich sind, hat der Vizepräsident des BSI in einer Bundestagsanhörung Anfang 2023 dargelegt: „Bevor überhaupt gesetzliche Regelungen zum staatlichen Umgang mit Schwachstellen geschaffen werden können, ist es hiesigen Erachtens notwendig, die Ziele, Definitionen und Rahmenbedingungen eines geplanten Schwachstellenmanagements festzulegen. So ist, rein auf Basis der Aussagen des Koalitionsvertrages, nicht klar, ob es sich bei dem Konzept um eine Art Coordinated Vulnerability Disclosure (CVD-Prozess), eine Art Vulnerabilities Equities Process (VEP), oder um beides inklusive darüberhinausgehender Maßnahmen handelt. [...] Die Pflichten des Staates zum Schutz der unterschiedlichen Grundrechte führen im Kontext der IT-Sicherheit und öffentlichen Sicherheit, wie am staatlichen Umgang mit Zero-Days deutlich wird, in einen Zielkonflikt staatlicher Sicherheitspolitik und damit innerhalb der Cybersicherheitsarchitektur Deutschlands, qua unterschiedlicher gesetzlicher Aufträge, auch zu einem Interessenkonflikt zwischen dem BSI und den Sicherheitsbehörden."[53] Mit dem BVerfG ist allerdings daran zu erinnern, dass es gerade deswegen, weil sich aus den objektiv-rechtlichen Gehalten der betroffenen Grundrechte keine ganz konkreten Regulierungsvorschläge ableiten lassen, Sache des Gesetzgebers ist, den „Zielkonflikt [...] zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken" andererseits aufzulösen.[54] Der Mangel an politischer Entschlusskraft kann Untätigkeit nicht entschuldigen. Zudem führt eine Auflösung des Zielkonflikts keineswegs in verfassungsrechtliche Aporien, sondern lässt sich mit den Bordmitteln rechtsstaatlicher Politikgestaltung lösen.

Orientierung geben insofern zunächst die vom Vizepräsidenten des BSI referenzierten Modelle, die hier kurz vorzustellen sind: So stellt das im Privatsektor entwickelte

---

[52] *SPD/Bündnis 90/Die Grünen/FDP*, Mehr Fortschritt wagen, 2021, S. 16: „Wir führen [...] ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen [...] ein". *BMI*, Zentrale Vorhaben des BMI 2023, 10.3.2023, S. 1, https://fragdenstaat.de/dokumente/237015-zentrale-vorhaben-des-bmi-2023/.

[53] Stellungnahme des BSI zum Fragenkatalog zur Öffentlichen Anhörung des Ausschusses für Digitales am 25.1.2023 zum Thema „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland", Ausschuss-Drs. 20(23)125, S. 11 f.

[54] BVerfG, NVwZ 2021, 1361, LS 2b.

CVD-Verfahren, auch bekannt als Responsible Disclosure, primär darauf ab, dass vor einer Veröffentlichung die betroffenen Unternehmen ausreichend Zeit haben, um die Lücke durch einen Patch oder sonstige Maßnahmen zu schließen, ohne die Notwendigkeit einer Veröffentlichung an sich in Abrede zu stellen.[55] Eine hieran orientierte Regelung muss dementsprechend vor allem sachangemessene Zeitintervalle für die Prüfung der Sicherheitslücken definieren. Demgegenüber ist das Modell des „Vulnerabilities Equities Process" (VEP) deutlich komplexer und verweist auf die in den USA etablierte Art und Weise des Umgangs staatlicher Stellen mit Schwachstellen. Dieses Modell wurde zuletzt 2017 überarbeitet und als „Vulnerabilities Equities Policy and Process" (VEP 2017) teilweise veröffentlicht.[56] Verschiedene Länder haben seither ähnliche Regularien verabschiedet.[57] Konkret hat der VEP zwei Regelungsebenen. Zum einen etabliert er ein klares Regel-Ausnahme-Verhältnis und definiert bestimmte (enge) Gründe, die das Absehen von einer Veröffentlichung rechtfertigen können. Nur dort, wo ein „demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes" vorliegt, dürfen Schwachstellen geheim gehalten werden.[58] Im Übrigen hat das öffentliche Interesse an IT-Sicherheit Vorrang.[59] Zum anderen etabliert der VEP einen strukturierten Prozess, den eine staatliche Behörde anstoßen muss, wenn sie eine Schwachstelle entdeckt hat. In diesem mehrstufigen Verfahren, das nicht bei einer einzelnen Behörde, sondern in dem unter Vorsitz des Präsidenten tagenden National Security Council (NSC) angesiedelt ist, werden dann die Interessen aller relevanten staatlichen Akteure – keineswegs nur der Nachrichtendienste – ermittelt.[60] Der Prozess mündet in einer Entscheidung darüber, ob die Lü-

[55] Hierzu und zum Gegenmodell einer „full disclosure" siehe https://en.wikipedia.org/wiki/Full_disclosure_(computer_security). Für den Umgang Privater mit Schwachstellen finden sich Grundregeln auch in ISO/IEC 30111:2013 Information technology – Security techniques – Vulnerability handling processes. Diese werden einfachrechtlich überlagert durch die Informations- und Meldepflichten des BSIG und weiterer Normen.

[56] *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, https://www.hsdl.org/c/abstract/?docid=805726.

[57] Siehe für Großbritannien: *GCHQ*, The Equities Process, 2018, https://www.gchq.gov.uk/information/equities-process; dazu *Weaver*, The GCHQ's Vulnerabilities Equities Process, Lawfare v. 3.6.2019, https://www.lawfaremedia.org/article/gchqs-vulnerabilities-equities-process. Für Australien: *Australian Signals Directorate*, Responsible Release Principles for Cyber Security Vulnerabilities, 2022, https://www.asd.gov.au/sites/default/files/2022-03/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf. Für die Union siehe *ENISA*, Coordinated Vulnerability Disclosure Policies in the EU, April 2022, https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

[58] Zur Prüfung, ob ein Interesse „overriding" ist, sind folgende Gesichtspunkte in die Abwägung einzustellen: „defensive, military, intelligence and operational, commercial, international relationships, and law enforcement", vgl. *White House* (Fn. 56), S. 1, 8 f. Diese Kategorien werden in Annex B (a. a. O., S. 13 f.) weiter charakterisiert.

[59] *White House* (Fn. 56), S. 1.

[60] Allerdings werden die Interessen von Militär und Nachrichtendiensten an verschiedenen Stellen im Prozess priorisiert und in Teilbereichen auch vom VEP ausgenommen, *White House* (Fn. 56), S. 9.

cke dem betroffenen Unternehmen mitgeteilt wird, damit dies Abwehrmaßnahmen ergreifen kann, oder ob der Staat die Lücke geheim hält, um sie für eigene Cyberaktivitäten zu nutzen. Während die durch den VEP 2017 vorgenommene Institutionalisierung des Schwachstellenmanagements weithin begrüßt wird, weist der Prozess im Detail zahlreiche Schwächen auf.[61]

II. Bausteine einer gesetzlichen Regelung des staatlichen Schwachstellenmanagements

Auch wenn die Modelle dem deutschen Gesetzgeber als erste Orientierung dienen können, dürfen weder das für den Privatsektor entwickelte CVD-Verfahren noch der stark den Besonderheiten der U.S.-Sicherheitsarchitektur verpflichtete VEP unreflektiert kopiert werden. Der deutsche Gesetzgeber muss vielmehr eigenständig eine Balance zwischen der grundgesetzlich radizierten Verantwortung des Staates für die IT-Sicherheit und legitimen Sicherheitsbelangen suchen. Erste Vorschläge dafür, wie ein staatliches Schwachstellenmanagement in Deutschland aussehen kann, wurden in der Wissenschaft entwickelt.[62] Im vorliegenden Zusammenhang sollen die fünf zentralen Bausteine dieser Regelung präsentiert werden.[63]

Erstens bedarf das Schwachstellenmanagement einer spezialgesetzlichen Grundlage. Eine Regelung des Verfahrens durch Innenrecht, wie dies beim VEP in den USA der Fall ist, oder durch eine untergesetzliche Norm genügt angesichts der hohen Grundrechtssensibilität der Materie nicht. Gerade bei potenten Sicherheitslücken, die auch für die Sicherheitsbehörden von Interesse sind, ist davon auszugehen, dass die Entscheidung über die Nichtoffenlegung für die dadurch berührten Grundrechte in aller Regel wesentlich ist.[64] Mit Blick auf die Einsatz-, Kollisions- und Proliferationsrisiken ist es zudem unzureichend, wenn – wie bisher – staatlichen Stellen „nur" der Einsatz von IT-Sicherheitslücken für bestimmte Zwecke erlaubt wird, etwa in den Befugnisnormen zur Quellen-TKÜ, ohne die Modalitäten der Nutzung näher zu regeln. Sinnvollerweise erfolgt diese Regelung in enger Abstimmung mit dem allgemeinen Informationssicherheitsrecht, da hier, etwa bei Meldepflichten, Pflichtenkollisionen vermieden werden müssen.[65]

---

[61] Vgl. Ambashta, Berkeley Tech. L. J. Blog v. 22.4.2019; Gaudion, It's Time to Reform the U.S. Vulnerabilities Equities Process War Room, 2.9.2021, https://warroom.armywarcollege.edu/articles/vep/; Thompson, Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter, Lawfare v. 13.1.2021, https://warroom.armywarcollege.edu/articles/vep/.

[62] Vgl. insbes. *Herpig* (Fn. 28); *Wischmeyer* (Fn. 6), S. 292 ff.

[63] Einer eigenständigen Untersuchung bedarf die Frage, wie sich staatliche Stellen überhaupt Kenntnis von IT-Sicherheitslücken verschaffen.

[64] Zum in der jüngeren Rechtsprechung gerade im Kontext digitaler Überwachungstechnik tendenziell weit interpretierten Wesentlichkeitskriterium siehe nur BVerfGE 134, 141 (184, Rn. 126); 139, 148 (174 f., Rn. 51); 141, 143 (170, Rn. 59 ff.) m. w. N.

[65] Dies wird insbesondere durch die jetzt durch die NIS 2-RL anstehende Einbindung staatlicher Stellen in das KRITIS-Regime relevant.

Zweitens ist im Gesetz ein eindeutiges Regel-Ausnahme-Verhältnis zu statuieren, um der überragenden Bedeutung des staatlichen Interesses an sicheren Informationsinfrastrukturen Rechnung zu tragen. In dieser Hinsicht kann der VEP als Vorbild dienen. Anders als im VEP sind demgegenüber Bereichsausnahmen, etwa für die Nachrichtendienste, nicht anzuerkennen, schon weil es für die durch die Bevorratung von Sicherheitslücken entstehenden Kollisions- und Proliferationsrisiken keinen Unterschied macht, durch welche staatliche Behörde bzw. im Kontext welcher staatlichen Aufgabe sie erzeugt werden.

Drittens muss das Gesetz Kriterien definieren, welche Art von Sicherheitslücken unter welchen Bedingungen wann und wem gegenüber offengelegt werden dürfen bzw. müssen. Um eine möglichst umfassende Interessenabwägung zu gewährleisten, sollte die Abwägung darüber hinaus in Grundzügen gesetzlich vorstrukturiert und die zu berücksichtigenden Faktoren benannt werden (etwa Zwecke der Nichtveröffentlichung, Schwere der Sicherheitslücke, besondere Interessen, Modalitäten der Veröffentlichung, Zero-Day- vs. N-Day-Schwachstellen, Grenzen der Abwägung etc.).[66] Um den Ausnahmecharakter einer Entscheidung zur Nichtveröffentlichung zu bekräftigen, sollte angeordnet werden, dass die durch die Geheimhaltung verfolgten verfassungsrechtlich radizierten Interessen in der Abwägung die Interessen an der Veröffentlichung wesentlich überwiegen müssen.

Angesichts der Proliferationsrisiken, die mit jeder Entscheidung über die Nichtveröffentlichung verbunden sind, muss die gesetzliche Regelung zum Schwachstellenmanagement *viertens* vorsehen, dass ein am jeweiligen Stand der Technik gemessen besonders hoher Informationssicherheitsstandard für die „Aufbewahrung" des Wissens über die Sicherheitslücken gewährleistet ist.[67] Dies muss durch transparente inneradministrative Kontrollmechanismen abgesichert werden.

Fünftens und letztens muss die gesetzliche Regelung die organisatorischen und prozeduralen Rahmenbedingungen des Offenlegungsprozesses definieren. Nicht anders als in anderen Gebieten des Verwaltungsrechts haben die institutionelle Verortung und die prozedurale Ausgestaltung wesentlichen Einfluss auf die Anwendung und die Effektivität der materiell-rechtlichen Vorgaben zur Schwachstellen-Governance.[68] Was die *Zuständigkeit* betrifft, muss der Prozess angesichts der großen und zudem ressortübergreifenden Bedeutung der Materie hierarchisch strukturiert werden und alle thematisch damit befassten Instanzen der Exekutive, bis hin zu deren Spitze, involvieren; dies erfordert eine entsprechende Hochzonung der Entscheidungszuständigkeit über

[66] Orientierung können hier bieten: Annex B zu *White House* (Fn. 56), S. 9; *Herpig* (Fn. 28), S. 23 ff.; *Wischmeyer* (Fn. 6), S. 297 ff.

[67] Vgl. BVerfGE 125, 260 (325 ff., Rn. 221 ff.); 155, 119 (205, Rn. 188).

[68] Zur Relevanz von Organisationsfragen allgemein *Möllers*, Materielles Recht – Verfahrensrecht – Organisationsrecht, in: Trute/Groß u. a. (Hrsg.), Allgemeines Verwaltungsrecht, 2008, S. 489 ff.

die Nichtveröffentlichung einer Sicherheitslücke.[69] Relevant ist zudem – wie bei jedem bedeutsamen und grundrechtsrelevanten exekutiven Entscheidungsverfahren – die *Kontrolle*.[70] Bei deren Ausgestaltung ist zu bedenken, dass die sensitive Natur des Verfahrensgegenstandes Geheimschutzmaßnahmen erforderlich macht, was die Kontrollmöglichkeiten notwendig erschwert.[71] Dies ist jedoch nicht die einzige Herausforderung, die das Schwachstellenmanagement unter dem Gesichtspunkt der Kontrolle bereitet. Hinzu kommt insbesondere die technische Dimension der Kontrollfrage, die gerade im öffentlichen Sektor bisher kaum vorhandene Expertise verlangt. Im Detail sind hier verschiedene inneradministrative, gerichtliche und parlamentarische Kontrollinstanzen sowie die Öffentlichkeitskontrolle in Stellung zu bringen.[72] Hierauf kann vorliegend nicht im Detail eingegangen werden; es soll nur erwähnt werden, dass dem Parlamentarischen Kontrollgremium auch in diesem Zusammenhang bei sensitiven Sicherheitsfragen eine Schlüsselrolle zukommen muss.

E. Schluss

Die verfassungsrechtliche Verantwortung des Staates für die Informationssicherheit verlangt nicht nur, dass der Staat Private in dieser Sache in die Pflicht nimmt und Regeln zur IT-Sicherheit trifft. Vielmehr muss er auch seinen eigenen Umgang mit IT-Sicherheitslücken daraufhin überprüfen, inwieweit er Risiken für Verfassungsgüter, insbesondere Grundrechte, erzeugt, und hierfür entsprechende Sicherungsmechanismen vorsehen. Konkret bedarf es, wie gezeigt, der gesetzlichen Einführung eines staatlichen Schwachstellenmanagements.

Dabei darf nicht übersehen werden, dass der rationalisierende Einfluss, den eine solche Regelung auf die Exekutive hat, nicht notwendig zu einer Einschränkung staatlicher Aktivitäten in diesem Bereich führen muss. Ein belastbares normatives Gerüst kann die Suche nach und das Management von IT-Sicherheitslücken vielmehr auch stimulieren. Nebenfolge einer Verrechtlichung wäre dann, dass die Exekutive Sicherheitslücken nicht weniger, sondern mehr nutzt. Umso wichtiger ist es, an dieser Stelle daran zu erinnern, dass die primären Anstrengungen des Staates der Hebung des allgemeinen

---

[69] Dazu, welche Institution hier konkret zur Steuerung in Frage kommen, siehe *Wischmeyer* (Fn. 6), S. 301 f.

[70] Zu den verfassungsrechtlichen Grundlagen der (Verwaltungs-)Kontrolle siehe nur *Kahl*, Kontrolle der Verwaltung und des Verwaltungshandelns, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 45 Rn. 66 ff.

[71] Hier sind gleichermaßen strategische, institutionelle und treuhänderische Geheimhaltungsgründe einschlägig; dazu und zur notwendigen Engführung exekutiver Geheimhaltungsinteressen ausführlich *Wischmeyer*, Die Verwaltung 51 (2018), 393.

[72] Differenziert dazu *Kahl* (Fn. 70), § 45 Rn. 79 ff. Zu den einzelnen Bausteinen von Kontrollrelationen *Kempny*, Verwaltungskontrolle, 2017, S. 16 ff.

IT-Sicherheitsniveaus gelten müssen. Nur im Kontext eines umfassenden und leistungsfähigen IT-Sicherheitsrechts lässt es sich überhaupt rechtfertigen, dass der Staat ausnahmsweise Sicherheitslücken zu eigenen Zwecken nutzt.

Kapitel 2: Effektive Rechtsdurchsetzung

Welche Befugnisse braucht das BSI, um IT-Sicherheitslücken bekämpfen zu können?

Steve Ritter

A. Einleitung

Auch wenn die Überschrift lediglich auf Befugnisse abstellt, wird der Beitrag nicht nur auf Befugnisse eingehen, da für die Bekämpfung von IT-Sicherheitslücken nicht immer Befugnisse benötigt werden. Zwar werden diese im Bereich der Sicherheitsgesetzgebung gerne gefordert, oftmals reichen aber auch schon Mandate. Solche Mandate hat auch das BSI bereits in vielen Bereichen. Nach einer kurzen Darstellung, was man unter IT-Sicherheitslücken verstehen kann, geht der Beitrag der Frage nach, welche Aspekte es bei deren Bekämpfung gibt. Denn der Begriff der Bekämpfung hört sich einfach an, besteht aber eigentlich aus mehreren Schritten bzw. Aspekten. Ein erster Schritt ist die Entdeckung von Lücken, die schon stark von rechtlicher Regulierung geprägt ist. Diese Regulierung weist neben Lösungen leider auch Probleme auf. Der zweite Schritt ist die Schließung von Lücken. Auch hier gibt es bereits rechtliche Regelungen. Hinzu tritt ein dritter Aspekt, der für die Zukunft sehr entscheidend sein wird: Was kann man eigentlich tun, um Lücken zu verhindern, und was tut das BSI an der Stelle bereits.

Zudem geht der Beitrag auf Regulierungsvorhaben im Bereich der IT-Sicherheit ein. Davon gibt es derzeit viele und einige könnten Lösungen für die Probleme bringen, über die im Zusammenhang mit IT-Sicherheitslücken derzeit noch nachgedacht wird.

B. Was sind eigentlich Sicherheitslücken?

Doch was sind eigentlich IT-Sicherheitslücken?

I. Sicherheitslücken in Hard- und Software

Wir denken bei Sicherheitslücken alle sofort an eine Software, die schlecht programmiert ist. Das kann ein Angreifer im Zweifelsfall ausnutzen, um in ein System einzudringen und die Kontrolle zu übernehmen. Doch IT-Sicherheitslücken gibt es auch in

Hardware. In den letzten Jahren wurden z.B. regelmäßig Sicherheitslücken in Prozessoren gefunden[1], also den in den Kernbestandteilen eines Computers, in denen die Datenverarbeitung abläuft. Es ist unrealistisch, dass jemand vorbeikommt und entweder den unsicheren Prozessor austauscht oder anfängt, darin Leiterbahnen auszulöten und neue zu verlegen, um die Sicherheitslücke zu beseitigen. Bisher war es bei Hardware-Sicherheitslücken oft möglich, die Lücken über Softwareupdates zu beheben. Das kann sowohl auf Ebene der Betriebssysteme und Anwendung passieren als auch über die Software, die auch in Prozessoren enthalten ist.[2] Das ging jedoch teilweise nur auf Kosten der Leistungsfähigkeit und der Funktionalität.[3] Bei solchen Lösungen stellt sich dann wieder die Frage nach der Definition des Mangelbegriffs, wenn der Prozessor dadurch plötzlich signifikant Leistung verliert. Aus IT-Sicherheitssicht ist dann jedoch die Hauptsache, dass die Lücke nicht mehr für Angriffe ausnutzbar ist.

Ähnliches gilt im Bereich der Software. Absolut fehlerfrei zu programmieren, ist enorm schwierig. Wer schon mal ein größeres wissenschaftliches Werk herausgebracht hat, weiß, wie schwierig es ist, sicherzustellen, dass kein einziger Zahlen- oder Buchstabendreher, Satzzeichenfehler oder Vertipper im Endergebnis enthalten ist. Und da reden wir über Werke, die für uns als Menschen, wenn wir sie lesen, sehr leicht verständlich sind. Das ist bei Quellcode von Software oft nicht der Fall. Da gibt es Interdependenzen innerhalb des Codes. Da taucht eine Variable auf, die zwei Millionen Zeilen Code weiter hinten befüllt wird, und aus dieser Zusammenarbeit der einzelnen Code-Bestandteile folgt dann der Programmablauf. Wenn in einzelnen Quellcode-Zeilen Fehler enthalten sind, können das Ansatzpunkte für Angreifer sein, um sie ausnutzen und im schlimmsten Fall Systeme zu übernehmen bzw. manipulieren. Diese Interdependenzen und die mangelnde Lesbarkeit sind schon gewichtige Probleme für die Vermeidung von Fehlern. Diese werden jedoch noch ergänzt durch den schieren Umfang des Quellcodes. Ein Vergleich kann die Dimension vielleicht etwas verdeutlichen: Das komplette Werk „Harry Potter“ soll ca. zehn Millionen Zeilen umfassen. Wer die Bücher gelesen hat, weiß, das zu lesen dauert schon recht lange. Wenn man sich dann vorstellt, dass heutzutage ein Betriebssystem oder die Software in einem Auto um die 100 Mio. Zeilen Code umfasst, der für uns Menschen selbst, wenn wir so eine Zeile lesen, nicht unmittelbar verständlich ist mit all seinen Auswirkungen und der Bedeutung im Programmablauf, dann wird sehr schnell klar, worin die Herausforderung liegt. Zwar

[1] Vgl. https://meltdownattack.com/ oder https://downfall.page/ (diese und alle anderen URLs zuletzt abgerufen am 13.12.2023).

[2] https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/best-practices/sysadmin-guidance-transient-execution-side-channel.html und https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7008.html.

[3] Vgl. https://www.microsoft.com/en-us/security/blog/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/.

gibt es auch Werkzeuge für die Analyse von Quellcode, aber auch die haben ihre Grenzen. Auch durch die Automatisierung lassen sich nicht alle Lücken verhindern.[4] Das Problem ist die Komplexität von Programmen im Ablauf.

Natürlich ist es möglich, Code zu schreiben, der genau das tut, was er soll, und der auch nur das tut, was er soll. Dazu werden sog. formale Methoden genutzt, die das mathematisch bzw. logisch garantieren.[5] Diese haben in den letzten Jahren deutliche Fortschritte gemacht. Waren es vor einigen Jahren nur wenige 10.000 Zeilen Code, sind es inzwischen mehrere zehntausend Zeilen Code, die so zu sicheren Programmen gebaut werden können. Jedoch ist das noch immer weit entfernt von den Größenordnungen, die viele moderne Anwendungen haben.[6] Ein Browser kann auch schon mal einen Umfang von 21 Mio. Zeilen Code haben.[7]

II. Fehlkonfigurationen

Eine zweite Quelle für Sicherheitslücken sind Fehlkonfigurationen. Diese gibt es sowohl in der Form, dass Systeme mit unsicheren Voreinstellungen ausgeliefert werden, oder in der Form, dass es den Nutzern schwerer als nötig gemacht wird, sie abzusichern. Rechtlich wirft das die Frage auf, ob in diesen Fällen ein Mangel vorliegt. Es gibt aber auch die Fehlkonfigurationen, bei denen Nutzer sichere Voreinstellungen bewusst ignorieren bzw. abändern und dadurch Sicherheitslücken schaffen, die für Angriffe missbraucht werden können. Ein Beispiel dafür sind etwa Cloud-Speicher, wie etwa sog. S3-Buckets. Das sind Cloud-Instanzen, die man buchen kann. Diese sind standardmäßig gesichert und man muss die Möglichkeit für einen Zugriff ohne Passwort für Dritte bewusst aktivieren[8], um eine neue Lücke zu schaffen. Gleichwohl gehen viele Datenlecks in den letzten Jahren darauf zurück, dass genau das erfolgt ist.[9] Anders als bei den bisher genannten Problemen gehen die Fehlkonfigurationen nicht auf (Un-)Tätigkei-

---

[4] Vgl. *Ayewah et al.*, Experiences Using Static Analysis to Find Bugs,S. 3 abrufbar über https://storage.googleapis.com/gweb-research2023-media/pubtools/pdf/34339.pdf; *Chatzieleftheriou/Katsaros*, Test-driving static analysis tools in search of C code vulnerabilities, abrufbar unter: http://delab.csd.auth.gr/papers/COMPSACW2011ck.pdf.

[5] Vgl. *Huisman/Gurov/Malkis*, Formal Methods: From Academia to Industrial Practice S. 2, abrufbar unter: https://wwwbroy.in.tum.de/~malkis/Huisman_Gurov_Malkis_-_Formal_Methods_From_Academia_to_Practice_A_Travel_Guide.pdf; *Woodcock et al.*, Formal Methods: Practice and Experience S. 2, abrufbar unter https://www.researchgate.net/profile/Peter-Larsen-13/publication/30421288_Formal_Methods_Practice_and_Experience/links/0deec521efe3e18d2d000000/Formal-Methods-Practice-and-Experience.pdf.

[6] Vgl. zu den Kompromissen bei großen Mengen Code auch *Woodcock et al*., Formal Methods: Practice and Experience S. 12.

[7] Vgl. https://hacks.mozilla.org/2020/04/code-quality-tools-at-mozilla/.

[8] Vgl. https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-access-control.html.

[9] Vgl. etwa https://techcrunch.com/2023/05/05/security-researcher-finds-trove-of-capita-data-exposed-online/; https://www.forbes.com/sites/thomasbrewster/2017/07/06/massive-wwe-leak-exposes-3-million-wrestling-fans-addresses-ethnicities-and-more/.

ten der Anbieter zurück, seien es Verkäufer oder auch einfach Diensteanbieter. Stattdessen sind die hier die Nutzer Ursache der IT-Sicherheitslücken. Als Folge können die Nutzer die von ihnen gespeicherten Daten „verlieren". Dritte können dann unberechtigt auf diese Daten zugreifen und sie verschlüsseln, löschen oder exfiltrieren. Angreifer können aber schlecht konfigurierte Systeme auch dafür nutzen, Angriffe auf die Systeme Dritter durchzuführen[10].

C. Bekämpfung von Sicherheitslücken

Nach der Feststellung, welche Arten von IT-Sicherheitslücken es gibt bzw. woraus sie resultieren, stellt sich die Frage, wie sie bekämpft werden können. Die Bekämpfung lässt sich wiederum grob in mehrere Aspekte unterteilen: Das Finden von Lücken, das Schließen von Lücken und auch das Verhindern von Lücken.

I. Lücken finden

Der erste Schritt ist die Erlangung von Kenntnis über das Vorhandensein von Lücken.

1. Rechtsrisiken bei der Suche nach Sicherheitslücken in Hard- und Software

In Bezug auf Lücken in Hard- und Software war das rechtlich gar nicht so einfach, auch für das BSI nicht. Denn schon die Untersuchung von Technik konnte einen strafbaren Eingriff etwa in Betriebs- und Geschäftsgeheimnisse nach § 17 Abs. 2 UWG a.F. darstellen. Deshalb hat sich das BSI vor ca. zehn Jahren sehr intensiv damit beschäftigt, welche Untersuchungen unter welchen Voraussetzungen für eine Behörde zulässig sind. Es stellte sich die Frage, ob man beliebig Hardware oder Software kaufen und dann nach allen Regeln der Kunst auseinandernehmen darf. Bei Hardware umfasst das auch die Frage, ob z.B. Chips abgeschliffen werden und mit ausgefeilter Technik daraufhin untersucht werden dürfen, wie sie im Inneren funktionieren. Solche tiefgehenden Untersuchungen waren vor zehn Jahren aufgrund der Grenzen des § 17 Abs. 2 UWG a.F. zum Schutz von Betriebsgeheimnissen nicht einfach. Man brauchte dafür eine Befugnis. Durch das Geschäftsgeheimnisgesetz hat sich dieses spezielle Problem inzwischen gelöst.

Darüber hinaus gibt es Regelungen im Strafrecht, die Untersuchungshandlungen mit einem Strafbarkeitsrisiko belasten. Hier wurde in der Vergangenheit im Zusam-

[10] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_042.pdf.

menhang mit IT-Sicherheitsmaßnahmen gerne der § 202c StGB als sog. „Hackerparagraf" genannt.[11] Eines der Hauptprobleme stellt aber tatsächlich der § 202a StGB dar. Dieser greift etwa, sobald man z.B. an obfuskierten Code gelangen möchte. Hersteller verschleiern ihren Quellcode (sog. code-obfuscation) teilweise, damit z.B. Konkurrenten den Maschinencode nicht über sog. reverse-engineering in lesbaren Quellcode umwandeln und untersuchen können. Da man damit einen Schutzmechanismus entfernt, ist das strafrechtlich ein Problem.[12] Für das BSI wurde deswegen im Jahr 2015 mit dem IT-Sicherheitsgesetz 1.0 und mit dem § 7a BSIG eine Befugnisnorm geschaffen, die als Rechtfertigungstatbestand für all diese Verbotsnormen wirkt.[13] Diese ist so ausgestaltet, dass das BSI nicht nur mit eigenen Mitarbeitern handeln, sondern auch Dritte hinzuziehen darf. Das ist wichtig, z.B. um auch fach- und produkttypische Expertise für spezielle Untersuchungen einbeziehen zu können. Mit der Schaffung des § 7a BSIG wurde das Problem aber nur für das BSI gelöst, während die Möglichkeiten aller übrigen Akteure der IT-Sicherheit damit deutlich zurückgeblieben sind[14]. Die IT-Sicherheitsforschenden außerhalb des BSI sehen sich bei ihrer Arbeit noch immer Rechtsrisiken ausgesetzt. Das ist deshalb ein Problem, da ein substanzieller Teil der IT-Sicherheitslücken von ethischen Hackern entdeckt wird.[15] Deshalb wird juristisch und mit den Sicherheitsforschenden die Frage diskutiert, wie Rechtssicherheit geschaffen werden kann, damit IT-Sicherheitslücken gesucht und entdeckt werden dürfen.[16] Das Bundesministerium des Innern, für Bau und Heimat adressierte dieses Problem in der Cybersicherheitsstrategie 2021.[17] Bis das Problem gelöst ist, versucht das BSI, die Sicherheitsforschenden auf andere Weise zu unterstützen, dazu später mehr. Für die eigenen Untersuchungen von Hard- und Software ist die Befugnis für Produktuntersuchungen nach § 7a BSIG jedoch sehr hilfreich.

2. Scannen nach Fehlkonfigurationen

Auch die Fehlkonfigurationen, also die zweite Klasse der o.g. IT-Sicherheitslücken, müssen erst einmal entdeckt werden, bevor man sie schließen kann. Mit dem IT-Sicher-

---

[11] Vgl. *Wagner/Vettermann et al.*, Verantwortungsvoller Umgang mit IT-Sicherheitslücken, S. 39, abrufbar unter: https://digitalrecht-oe.uni-trier.de/index.php/droe/catalog/view/9/8/59.

[12] Vgl *Wagner/Vettermann et al.*, Verantwortungsvoller Umgang mit IT-Sicherheitslücken, S. 37 f. *Brodowski/Golla* in: White Paper zur Rechtslage der IT-Sicherheitsforschung, S. 9 f.; abrufbar unter: https://www.fzi.de/wp-content/uploads/2021/11/doku-position-itsicherheitsforschung.pdf.

[13] *Ritter* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 52; *Wagner/Vettermann et al.*, Verantwortungsvoller Umgang mit IT-Sicherheitslücken S. 26.

[14] Vgl. *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 332.

[15] *Wagner/Vettermann et. al.*, Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, S. 19 f.

[16] Das BSI hat dazu bereits 2020 eine Dialog-Veranstaltung durchgeführt: https://www.bsi.bund.de/dok/13690916.

[17] Cybersicherheitsstrategie für Deutschland 2021 S. 46, abrufbar unter https://bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf.

heitsgesetz 2.0 wurde mit § 7b Abs. 1 BSIG die Befugnis des BSI eingeführt, nach Sicherheitslücken zu scannen. Das BSI kann also anlassbezogen danach suchen, ob Systeme fehlkonfiguriert sind oder ein Softwarestand eingesetzt wird, für den es zwar Patches gibt, die aber nicht eingespielt sind, so dass die Systeme angreifbar sind. Die Befugnis ist bisher leider so ausgestaltet, dass das BSI dies nur bei wenigen Stellen darf. Dazu zählen die Bundesverwaltung, Betreiber Kritischer Infrastrukturen i.S.d. § 2 Abs. 10 BSIG, Anbieter digitaler Dienste i.S.d. § 2 Abs. 12 BSIG und Unternehmen im besonderen öffentlichen Interesse i.S.d. § 2 Abs. 14 BSIG. Die IP-Adressen der zu scannenden Systeme müssen diesen Stellen zudem auf einer sog. Weißen Liste zugeordnet sein, § 7b Abs. 1 S. 2 BSIG. Die so ausgestaltete Scan-Befugnis erzeugt einen gewissen bürokratischen Aufwand und ist daher nicht unbedingt praktikabel.[18] Zudem sind die Stellen, deren Systeme gescannt werden können, durchaus wichtige Stellen. Aber es gibt in Deutschland deutlich mehr Nutzer von IT, bei denen IT-Sicherheitslücken Schäden sowohl für diese Nutzer als auch für Dritte verursachen können. Dienstleister, die das ohne staatlichen Auftrag machen, die scannen auch heute schon mehr. Nur die staatliche Behörde, die dafür zuständig ist, darf es bisher nicht im wünschenswerten Umfang. Daher wäre es sinnvoll, wenn das BSI im gesamten deutschen IP-Adressraum scannen dürfte, um die Systembetreiber auf die IT-Sicherheitslücken hinweisen zu können, damit sie geschlossen werden. Bereits heute sieht § 7b Abs. 3 BSIG diese Information der für das System Verantwortlichen als Zweck der Scans vor. Möglichen Bedenken zur erweiterten Datensammlung durch eine Sicherheitsbehörde bei einer Erweiterung der Scan-Befugnis könnte man regulatorisch durch eine noch konkreter ausformulierte Zweckbindung für die so erlangten Informationen begegnen.

Juristisch interessant ist, dass § 7b Abs. 1 BSIG von „Port Scans“ spricht. Port Scans funktionieren – stark vereinfacht ausgedrückt – so, dass einem System Datenpakete geschickt und die Antworten des Systems analysiert werden. Das ist für sich genommen schon kein Grundrechtseingriff. Dafür braucht man keine Befugnis. [19] Erst die Gesetzesbegründung stellt klar, dass der Gesetzgeber dem BSI mit § 7b BSIG durchaus mehr Scantiefe erlaubt hat.[20] Norm und Begründung fallen insoweit ein Stück weit auseinander. Jedoch lässt sich das Problem, wie so oft, im Rahmen der Auslegung handhaben. Gleichwohl wäre eine Klarstellung des Gesetzeswortlautes gepaart mit einer Ausweitung des Kreises der Stellen, deren Systeme gescannt werden dürfen, wünschenswert.

[18] Kritisch zur Praktikabilität auch *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 355 ff.

[19] Vgl. *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 362.

[20] Vgl. *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 363.

3. IT-Sicherheitsforschung

Wie bereits zuvor geschrieben, konnten die Rechtsrisiken im Zusammenhang mit der Untersuchung von Hard- und Software bisher nur für das BSI sehr weitgehend gelöst werden. Für die Sicherheitsforschenden außerhalb des BSI bestehen diese jedoch weiterhin.[21] Das Aufdecken aller IT-Sicherheitslücken schafft eine Behörde jedoch nicht allein. Die meisten Lücken werden von externen Sicherheitsforschenden entdeckt. Diese gehen mit der Meldung an Hersteller oder IT-Nutzer jedoch oft das Risiko ein, dass gegen sie Strafanzeige erstattet wird und die Polizei im Rahmen der Ermittlungen ihre gesamte IT einsammelt.[22] Unter diesen Bedingungen ist es nachvollziehbar, dass Lücken aus Angst ungern gemeldet werden. Auch hier bietet sich das BSI als Cybersicherheitsbehörde an. Denn nach § 4b Abs. 2 BSIG nimmt das BSI Informationen, z.B. zu Sicherheitslücken, auch anonym entgegen Diese Regelung dient gerade dem Ziel, den Meldenden das Risiko der Strafbarkeit zu nehmen, welches sich aus der Meldung von IT-Sicherheitsinformationen ergibt.[23] In der Folge kann das BSI einen organisatorischen Rahmen dafür bieten, dass IT-Sicherheitsforschende diese Informationen an das BSI melden, mit der Bitte auf den Hersteller zu zugehen. Diese Möglichkeit wird regelmäßig wahrgenommen. Die Meldenden, die auf Anonymität verzichten wollen, haben bei erfolgreichen Meldungen an das BSI die Möglichkeit, in einer Art Hall of Fame namentlich gewürdigt zu werden.[24]

II. Das Schließen von Lücken

Nach dem Finden von Lücken steht deren Schließung an. Diesbezüglich gibt es eine ganze Reihe von rechtlich regulierten Instrumenten, auf die das BSI zurückgreifen kann.

1. CVD-Prozess – das Schließen beim Hersteller

Es wird ein sogenannter Coordinated Vulnerability Disclosure Prozess (CVD-Prozess) angestoßen, das heißt eine koordinierte und strukturierte Offenlegung der Lücke gegenüber den betroffenen Herstellern. Damit informiert man den Hersteller, dass eine Lücke entdeckt wurde, worin die Lücke besteht und ggf. welche weiteren Informationen es gibt, um die Lücke zu prüfen, zu verstehen und am Ende vor allem auch zu schließen.

---

[21] Vgl. *Wagner/Vettermann et al.*, Verantwortungsvoller Umgang mit IT-Sicherheitslücken, S. 37; *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 332.

[22] https://www.golem.de/news/sicherheitsluecke-gemeldet-modern-solution-bringt-it-experten-nun-doch-vor-gericht-2308-176827.html.

[23] Vgl. *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 191.

[24] https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Hall_of_Fame/Hall_of_Fame_node.html.

Wie bei allen Meldungen an Hersteller kann es auch im Anschluss an eine vom BSI eingereichte Meldung noch zu Diskussionen kommen. Das kann z.B. der Fall sein, wenn der Hersteller Lücken nicht nachvollziehen kann, deren Schließung für zu zeitaufwendig hält oder gemeinsam deren Schwere diskutiert werden muss. Dann muss im Rahmen der Diskussion durch das BSI geprüft werden, ob es wirklich so komplex ist, diese Lücke zu schließen, bevor es weitere Maßnahmen ergreift. Dabei ist das Problem oft, dass es nicht nur darum geht, z.B. Fehler im Code zu beseitigen. Vielmehr muss man sich die Software und die Sicherheitslücke genau ansehen, um sicherzustellen, dass erste auch nach der Beseitigung der gemeldeten Schwachstelle auch noch zuverlässig funktioniert. Denn es bringt nichts, wenn zwar die Lücke geschlossen wird, aber etwa eine Software nach dem Sicherheitsupdate die ihr zugedachte Funktion, z.B. im Zusammenspiel mit anderen IT-Produkten in komplexen IT-Systemen, schlicht nicht mehr erfüllt.[25] Die Kompatibilität mit anderen Komponenten in den IT-Landschaften soll gerade aufrechterhalten bleiben. Deswegen kann es manchmal technisch notwendig sein, sehr viel Arbeit zu investieren, bevor ein Sicherheitsupdate veröffentlicht wird.

Sofern sich in den Diskussionen zwischen Herstellern und BSI herausstellt, dass der Hersteller sich querstellen und die Lückenschließung blockieren möchte, kommt der Punkt, an dem über eine Warnung der Nutzenden gem. § 7 Abs. 1 BSIG nachgedacht werden muss. Diese Warnungen des BSI dienen vorrangig der Information der Öffentlichkeit, damit diese sich vor den IT-Sicherheitslücken schützen können, etwa indem sie Absicherungsmaßnahmen ergreifen. Neben der Informationsfunktion ist mit der Warnung aber auch ein Pranger-Effekt verbunden. Dieser macht die Warnung auch zu einem wirkungsvollen Durchsetzungsinstrument des BSI. Warnmeldungen des BSI werden nicht nur von Medien in Deutschland, sondern auch im Ausland aufgegriffen.[26] Das macht sie zu einem sehr effektiven Mittel, wenn es um Hersteller im Ausland geht, die sich dem klassischen Verwaltungszwang deutscher Behörden aufgrund ihres Sitzes im Nicht-EU-Ausland ansonsten entziehen können.

Doch auch klassische Verwaltungsmaßnahmen kann das BSI ergreifen. So darf es etwa bei IT-Sicherheitsvorfällen im Bereich der Bundesverwaltung, der Betreiber Kritischer Infrastrukturen oder von Unternehmen im besonderen staatlichen Interesse anordnen, dass die Hersteller der eingesetzten Produkte an der Vorfallbeseitigung mitwirken (§ 5b Abs. 6 BSIG und § 8b Abs. 6 BSIG). Dahinter steht der Gedanke, dass oftmals nur die Hersteller Sicherheitsupdates für IT-Sicherheitslücken in ihren Produkten bereitstellen können und IT-Sicherheitsvorfälle bei den genannten Stellen durchaus auf

[25] Solche Probleme treten durchaus auf: vgl. https://www.t-online.de/digital/aktuelles/id_100160458/nach-sicherheits-update-windows-11-nutzer-melden-massive-probleme-.html.

[26] Etwa die Warnung vor der Log4j-Schwachstelle: https://www.reuters.com/technology/german-cybersecurity-watchdog-issues-red-alert-warning-software-2021-12-12/.

solche IT-Sicherheitslücken zurückgehen können.[27] Das ist ein verwaltungsformaler Prozess. Es muss u.U. ein Bescheid in das Nicht-EU-Ausland, etwa nach China, geschickt werden. Gerade im internationalen und Jurisdiktionen überschreitenden Bereich kann man sich die Erfolgschancen und vor allem die Geschwindigkeit eines solchen Vorgehens gut ausmalen.[28] Daher wurde dieses Mittel bisher auch noch nicht genutzt, sondern andere Wege wie die Warnung oder deren Androhung als wirksamere Mittel ergriffen.

2. Schließung auf Seiten der Verwender

Um Lücken in aktiv genutzten IT-Systemen oder -Produkten zu schließen, ist der Hersteller nur ein möglicher Akteur. Sofern Einigkeit über die Existenz einer IT-Sicherheitslücke besteht, reagieren Hersteller auch für gewöhnlich mit der Bereitstellung von Patches. Falls nicht, dann spricht das BSI die Warnung aus, wenn andere Maßnahmen zur Erreichung des Ziels, der Erhöhung der IT-Sicherheit, nicht möglich sind.

a. Unpatchbare Produkte

Ein Beispiel dafür ist, wenn IT-Sicherheitslücken systembedingt im Produkt nicht schließbar sind und daher die Nutzenden angesprochen werden müssen. Diesen Fall gab es bei einem elektronischen Türschloss.[29] Dieses enthielt in bestimmten Baureihen eine Sicherheitslücke. Das Schloss war jedoch so konstruiert, dass es keine Update-Möglichkeit gab. In diesen Fällen blieb nur eine öffentliche Warnung nach § 7 BSIG, um die Nutzenden über die Lücke zu informieren, damit diese (zusätzliche) Sicherheitsmaßnahmen ergreifen können.

b. Nichteinspielen von IT-Sicherheitspatches und neueren Softwareversionen

Ein weiterer Fall, in dem die Schließung einer Lücke nicht mehr von Hersteller abhängt, ist, wenn zur Verfügung stehende Sicherheitsupdates nicht eingespielt werden. Im Jahr 2014 wurde das empirisch untersucht mit dem Ergebnis, dass damals zehn Sicherheitslücken für 97% der Angriffe verantwortlich waren und es für diese zehn Lücken bereits IT-Sicherheitspatches gab - sie wurden nur nicht eingespielt.[30] Auch Monate nach War-

---

[27] Vgl. BT-Drs. 18/5121, 16; *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 264

[28] *Hessel/Potel* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 8b BSIG Rn. 24. Kritisch zur Durchsetzbarkeit von Anforderungen aus dem kalifornischen Gesetz zur Sicherheit vernetzter Geräte gegenüber Herstellern in fremden Jurisdiktionen auch schon *Ritter*, MMR 2019, 3.

[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/Archiv/2022/BSI_W-005-220810.html.

[30] Vgl. Verizon Data Breach Report 2015, S. 16.

nungen des BSI blieben Schwachstellen in Exchange-Systemen offen, obwohl Software-Versionen ohne diese Lücke bereits zur Verfügung standen. In Deutschland betraf das mit 8.000 Systemen durchaus eine substanzielle Menge.[31] Das BSI warnt nicht nur vor den eigentlichen Lücken, sondern sammelt auch aus verschiedenen Quellen Informationen darüber, welche Systeme in Deutschland öffentlich einsehbar verwundbar sind, weil wichtige Sicherheitsupdates nicht, eingespielt wurden. Grundlage dieser Informationssammlung ist die Aufgabe aus § 3 Abs. 1 S. 2 Nr. 2 BSIG. Anhand dieser Informationen darf das BSI dann auf Basis des § 7 Abs. 1 BSIG die Betroffenen über die Verwundbarkeit ihrer Systeme warnen. Dafür darf das BSI gem. § 7 Abs. 1 S. 2 BSIG auch Informationsintermediäre nutzen. Das ist oft notwendig, da das BSI selbst nur IP-Adressen verwundbarer Systeme in Deutschland sieht, diese aber oftmals mangels weiterer Informationen keiner natürlichen oder jurstischen Person zuordnen kann. Es kann aber den Internet-Service-Provider (ISP) identifizieren, der wiederum weiß, welche seiner Kunden hinter einer IP-Adresse stecken. Über das sogenannte Provider-Informationssystem informiert das BSI dann den ISP über unsichere IT-Systeme aus seinem IP-Adressbereich und dieser kann dann seine Kunden informieren, so dass sie Absicherungsmaßnahmen ergreifen können. Leider nutzen die Kunden diese Informationen auch nicht immer, sondern sind der Meinung, ihr System laufe ja reibungslos. Gerade beim Hosting stellt sich dann die Frage, wer ist der Anbieter der jeweiligen Telemedien. Das können sowohl die Kunden als auch deren Hostinganbieter sein.[32] Gegenüber den Anbietern kann das BSI nämlich zur Abwehr von konkreten Gefahren für eine Vielzahl von Nutzern Anordnungen gem. § 7d BSIG erlassen bzw. sie zuvor darauf hinweisen, dass sie verpflichtet sind, ihre Systeme gegen Störungen abzusichern. Dabei ist es unerheblich, ob die Störung zu Problemen bei den Anbietern der Telemedien führt oder nur Probleme für Drittsysteme hervorrufen kann.[33] Es kommt häufig vor, dass Server so konfiguriert sind, dass zwar keine Gefahr für die Betreiber selbst besteht, die Systeme aber in einer Weise arbeiten, dass sie sich sehr gut für Angriffe auf Dritte instrumentalisieren lassen, zum Beispiel für sogenannte DDoS-Angriffe oder für die Verteilung von Schadsoftware. Für DDoS-Angriffe kann das etwa so ablaufen, dass ein Angreifer mit einer (oder mehreren) falschen Absender-IP-Adresse ein sehr kleines Paket an die schlecht konfigurierten Systeme schickt, welche diese mit sehr vielen und sehr großen Paketen an die vermeintliche Absender-IP-Adresse beantworten. Dabei handelt

[31] Vgl. den Tweet von CERT-Bund dazu unter: https://twitter.com/certbund/status/1460942013256323072.

[32] *Ritter* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 44 noch zu § 13 Abs. 7 TMG. Zur Abgrenzung der Verantwortlichkeiten vgl. *Eckhardt/Lepperhoff* in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 19 Rn. 75.

[33] Vgl. *Zwerschke* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 19 Abs. 4 TTDSG Rn. 3; *Eckhardt/Lepperhoff* in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 19 Rn. 83; vgl. *Paschke* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 432.

es sich um die IP-Adresse des Opfersystems. Man kann es sich wie mit einem Briefkasten vorstellen, bei dem so Millionen Pakete und Millionen Briefe in kurzer Zeit eingeliefert werden. Eine Unterscheidung nach valider Post, die wirklich gelesen werden müsste, und der falschen Post funktioniert dann nicht mehr, so dass der Briefkasten faktisch unbenutzbar wird. Auch bei Servern ist ein normaler Betrieb ab einer gewissen Menge an Paketen nicht mehr möglich und die Systeme dann irgendwann nicht mehr erreichbar. Um so etwas zu verhindern, ist es wichtig, dass auch die betroffenen Betreiber unsicherer Telemedien-Systeme tätig werden. Die dahingehende Absicherungspflicht für Anbieter von Telemedien resultierte aus dem mit dem 1. IT-Sicherheitsgesetz eingeführten § 13 Abs. 7 TMG a.F. und findet sich jetzt in § 19 Abs. 4 TTDSG.[34] Da die Nichtbefolgung der Anordnung nach § 7d BSIG zur Vornahme der Absicherungsmaßnahmen nach § 19 Abs. 4 TTDSG in § 14 Abs. 2 Nr. 1 lit. a BSIG bußgeldbewehrt ist, kann das BSI auch darüber einen Anreiz setzen, IT-Sicherheitsupdates einzuspielen oder die Systeme zu einem sicheren Betrieb umzukonfigurieren.

Sofern auch diese Anordnung nicht zum Erfolg führt, kann das BSI auch an die TK-Diensteanbieter herantreten und sie zur Umleitung des mit einem Angriff zusammenhängenden Datenverkehrs auffordern. Das dürfen die Betreiber nach § 169 Abs. 6 und 7 TKG auch ohne Anordnung machen. Tun sie das nicht, darf das BSI sie jedoch im Einvernehmen mit der BNetzA nach § 7c Abs. 1 S. 1 Nr. 1 BSIG dazu auch anweisen, um eine konkrete Gefahr z.B. für die Kommunikationstechnik des Bundes, eines Betreibers Kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse, eines Anbieters digitaler Dienste oder für Informations- und Kommunikationsdienste[35] abzuwenden. Die TK-Diensteanbieter müssen dann z.B. sog. Walled Gardens für die entsprechenden Kunden einrichten. Versuchen die Kunden dann ins Internet zu gehen, bekommt sie nur eine Vorschaltseite des TK-Diensteanbieters zu sehen, auf der sie über die bestehende Sicherheitslücke auf ihren Systemen und Möglichkeiten zur Schließung der Lücke hingewiesen werden. Wird die Lücke geschlossen, darf der Kunde wieder normal ins Internet kommunizieren.

Eine weitere Möglichkeit, zu der das BSI Provider nach § 7c Abs. 1 S. 1 Nr. 1 BSIG anweisen kann, ist die Einrichtung von sog. Sinkholes. Wird feststellt, dass Systeme aufgrund von IT-Sicherheitslücken von Angreifern zum Teil eines Botnetzes gemacht wurden und sich an Angriffen beteiligen, können auch die Verbindungen zwischen dem Botnetz und den Kundensystemen umgeleitet werden. Kennt man die IP-Adresse des Angreifers bzw. seines Command- and Control-Servers, kann man sämtliche Datenpakete, die dorthin übermittelt werden sollen, auf einen Sinkhole-Server umleiten.[36]

---

[34] *Eckhardt/Lepperhoff* in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 19 Rn. 83.

[35] Zur Reichweite des weitgehend unkonturierten Begriffs der Informations- und Kommunikationsdienste vgl. *Ritter* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 7c BSIG Rn. 20.

[36] Vgl. *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 400 f.

So können die unsicheren Systeme, die mit dem Sinkhole-Server kommunizieren wollen, identifiziert werden. Denn alle unsicheren Systeme, die Teil des Botnetzes sind, kommunizieren dann nicht mehr mit dem Server des Angreifers, um sich neue Angriffsbefehle abzuholen oder Daten dorthin auszuleiten, sondern mit einem System des BSI. Das BSI kann die Betreiber der Systeme wieder über das Provider-Informationssystem darüber informieren, dass sie infiziert sind und wahrscheinlich eine Sicherheitslücke in ihrem System haben, die sie schließen sollen.

Als weitere Befugnis hat das BSI mit § 7c Abs. 1 S. 1 Nr. 2 BSIG mit dem IT-Sicherheitsgesetz 2.0 die Möglichkeit erhalten, die TK-Diensteanbieter anzuweisen, technische Befehle zur Bereinigung von einem konkreten Schadprogramm an IT-Systeme der Nutzer zu übermitteln und so letztlich die Systeme auch von Lücken zu bereinigen. Im Hinblick auf das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist das sicherlich eine sehr spannende Norm. Denn letztlich erlaubt sie dem BSI einen Eingriff in genau dieses Grundrecht[37], das das BVerfG mit seiner Entscheidung von 2008 nicht nur entdeckt, sondern aufgrund der Rechtfertigungsanforderungen auch besonders hoch gewichtet hat. Denn Eingriffe in dieses Grundrecht sollen nach der Rspr. des BVerfG nur für überragend wichtige Schutzgüter zulässig sein. Daher wird in der Lit. durchaus die Frage aufgeworfen, ob diese Anordnungsbefugnis verfassungskonform ist.[38] Es dürfte jedoch durchaus einen – zwar engen – aber doch verfassungskonformen Anwendungsbereich geben. Und zwar dort, wo die Maßnahme dem Schutz eben jener vom BVerfG genannten Schutzgüter dient. Wo die Grenzen im Detail liegen, ist sicherlich mangels Rechtsprechung noch nicht im Detail klar. Wichtig ist jedoch auf Anwendungsebene die Berücksichtigung der Möglichkeit von Kollateralschäden. Deren Minimierung ist rechtlich geboten. Man kennt i.d.R. nicht die komplette IT-Umgebung, auf die mit der Übermittlung von Bereinigungsbefehlen eingewirkt wird, so dass das Risiko von Kollateralschäden real ist. Es muss also sehr vorsichtig vorgegangen und geprüft werden, was für Systeme das sind, wie sicher sie sind und mit welchem Maß an Sicherheit man davon ausgeht, dass die Befehle, die übermittelt werden sollen, tun was sie sollen, aber eben auch nur das.

III. Verhinderung von IT-Sicherheitslücken

Während die Schließung von Lücken durch das BSI in rechtlicher Hinsicht stark von Befugnissen geprägt wird, stellt sich bei der Verhinderung oft die Frage, ob nicht eine gesetzliche Aufgabe schon ausreicht.

[37] Anders die Gesetzesbegründung BT-Drs. 19/26106, 74, die durch *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 409 diesbezüglich kritisch hinterfragt wird.

[38] *Keppeler* in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes Rn. 411.

1. Cybersicherheitsempfehlungen

So gehört es etwa zu den Aufgaben des BSI, Hersteller und Anwender in Fragen der IT-Sicherheit zu beraten (§ 3 Abs. 1 S. 2 Nr. 14 BSIG). Im Rahmen dieser Beratung gibt es auch einen Dialog mit Herstellern und Akteuren im Bereich der Software und Hardware, bei dem das BSI auch Empfehlungen zur Absicherung der Produkte gibt. So wurde Browserherstellern etwa frühzeitig empfohlen, Sandboxing-Techniken in ihren Produkten zu implementieren.[39]

Auch für Anwender veröffentlicht das BSI regelmäßig Cybersicherheitsempfehlungen[40], in denen z.B. kleinen und mittleren Unternehmen (KMU) erläutert wird, wie sie ihre Systeme konfigurieren müssen, damit sie eine möglichst kleine Angriffsfläche haben – die KMU also mit der Konfiguration keine Lücken aufmachen.[41] Solche Empfehlungen gibt es vom BSI für viele Bereiche, z.B. auch für KI[42], Rechenzentrumsicherheit[43] oder Industrielle Steuerungs- und Automatisierungssysteme[44]. So hat das BSI etwa im Bereich der KI in diesem Jahr auf eine neue Klasse von Lücken und von Fehlerquellen, die sogenannten Indirect Prompt Injections, hingewiesen und erste Empfehlungen für den Umgang damit gegeben.[45] Empfehlungen sind ein sehr praktisches Instrument, da viele zwar IT-Sicherheit schaffen wollen, oft aber nicht wissen, was sie dafür tun müssen. Die Vermittlung des nötigen Wissens ist daher ein starker Hebel, um IT-Sicherheitslücken zu verhindern.

2. Standardisierung und Normung

Ein weiterer Ansatz zur Verhinderung von IT-Sicherheitslücken können die Standardisierung und Normung sein. Viele gesetzliche Verpflichtungen zu technischen oder organisatorischen Maßnahmen im Bereich der IT-Sicherheit stellen letztlich auf den

---

[39] Vgl. etwa die resultierende BSI-Empfehlung (BSI-E-CS 003, Version 1.1 vom 11.04.2012) an Endnutzer, auf Browser mit entsprechenden Techniken zu setzen. Abrufbar über https://web.archive.org/web/20121225071725/https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Empfehlungen/produktkonfiguration/BSI-E-CS-003.html.

[40] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/informationen-und-empfehlungen_node.html.

[41] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_KMU.pdf.

[42] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html.

[43] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/hochverfuegbarkeit_node.html.

[44] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/industrielle-steuerungs-automatisierungssysteme_node.html.

[45] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249034-1032.pdf. Diese technisch-rechtlich einordnend: *Ritter*, RDV 2023, 304.

Stand der Technik ab. Dieser wird u.a. durch nationale oder internationale Normen oder Standards beeinflusst bzw. konkretisiert.[46] Und auch hier folgt aus der gesetzlichen Beratungsaufgabe (§ 3 Abs. 1 S. 2 Nr. 14 BSIG) des BSI, sowie der Aufgabe, Sicherheitsvorkehrungen zu entwickeln (§ 3 Abs. 1 S. 2 Nr. 3 BSIG), ein Mandat für das BSI, im Bereich der Standardisierung und Normung tätig zu werden. Und dieses Mandat nimmt das BSI in verschiedensten nationalen und internationalen Standardisierungs- und Normungsgremien wahr, um die Aspekte der IT-Sicherheit in Standards und Normen einzubringen und damit IT-Sicherheitslücken in der Informationstechnik vorzubeugen. Zudem veröffentlicht es auch eigene Standards wie die BSI-Standards 200-1, 200-2. 200-3 und 200-4, die es kostenlos zur Verfügung stellt.[47] Das BSI veröffentlicht auch für Cloud Computing oder Künstliche Intelligenz (KI) eigene Standards. Es gibt den sog. BSI C5, d.h. den „Cloud Computing Compliance Criteria Catalog", der Mindestanforderungen an den sicheren Betrieb von Clouds aufstellt. Hier bekommen Anwender Hinweise, was aus Sicht der IT-Sicherheit zu beachten ist, wenn man einen Cloud-Dienstleister beauftragt. Im Bereich der künstlichen Intelligenz gibt es mit dem „AI Cloud Service Compliance Criteria Catalogue" (AIC4)[48] eine Orientierungshilfe für den sicheren Einsatz von KI und die Vermeidung von IT-Sicherheitslücken.[49]

Gerade die BSI-eigenen Standards sind ein gutes Beispiel dafür, wie Standards für Informationssicherheit den Anwendern durch das BSI auch leichter zugänglich gemacht werden können. Denn die in Standardisierungs- oder Normungsgremien erarbeiteten Werke müssen von Anwendern erst einmal bezahlt werden, um Einblick in den jeweiligen Standard oder die Norm zu erhalten.

Das BSI berät außerdem auch andere Behörden in Fragen der Sicherheit der Informationstechnik, wenn es um die Erarbeitung technischer Anforderungen geht, wie etwa das Kraftfahrtbundesamt im Bereich des autonomen Fahrens. Das entsprechende gesetzliche Mandat ist in § 1i Abs. 3 StVG enthalten.

3. Zertifizierung

Ein weiteres Werkzeug zur Vermeidung von IT-Sicherheitslücken ist die Zertifizierung. Auch Zertifizierung führt nicht zu 100% sicheren Produkten. Aber die vorherige Definition von Kriterienkatalogen mit Sicherheitszielen und zu ergreifenden Maßnahmen

[46] *Fischer* in: Hornung/Schallbruch, IT-Sicherheitsrecht, Kap. 13 Rn. 70. *Ritter* in: Kipker, Cybersecurity-HdB 2. Aufl., Kap. 15 Rn. 47.

[47] *Ritter* in: Kipker, Cybersecurity-HdB 2. Aufl.,Kap. 15 Rn. 48.

[48] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.pdf.

[49] *Ritter* in: Kipker, Cybersecurity-HdB2. Aufl., 2. Aufl.,Kap. 15 Rn. 50.

in Verbindung mit der anschließenden Prüfung, ob IT diese aufgestellten Anforderungen erfüllt[50], kann dennoch einen wichtigen Beitrag dazu leisten, IT-Sicherheitslücken zu vermeiden. Daher ist dem BSI auch in § 3 Abs. 1 S. 2 Nr. 4 BSIG die Aufgabe zugewiesen worden, die Sicherheit von informationstechnischen Systemen oder Komponenten zu prüfen und zu bewerten und Sicherheitszertifikate zu erteilen. Um diese Aufgabe wahrnehmen zu können, hat das BSI jedoch mit § 9 BSIG auch eine entsprechende Befugnis erhalten, da die Zertifizierung in Form von Verwaltungsakten erfolgt.[51] Dabei können Zertifizierungsverfahren unterschiedliche Grade an Sicherheit abbilden. Der Europäische Cyber Security Act (CSA), also die Verordnung (EU) 2019/881, der erstmals europäische Schema für die Cybersicherheitszertifizierung etablieren und damit die nationalen Zertifizierungsschemata ablösen soll, kennt dafür z.B. die Vertrauenswürdigkeitsstufen „niedrig", „mittel" oder „hoch" (Art. 52 CSA). Je höher das geforderte Maß an Sicherheit, desto größer ist jedoch auch der Prüfaufwand und desto teurer wird ein Zertifizierungsverfahren. Insbesondere Sicherheitslücken werden im Bereich der europäischen Zertifizierung durch den CSA ab der Vertrauenswürdigkeitsstufe „mittel" besonders adressiert. Denn ein nach dieser Stufe zertifiziertes Produkt darf keine bereits allgemein bekannten Sicherheitslücken enthalten und muss auch das Risiko von erfolgreichen Angriffen seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen klein halten, vgl. Art. 52 Abs. 6 CSA. In der Stufe „hoch" geht es dann schon darum, dass nicht nur bekannte Sicherheitslücken ausgeschlossen werden, sondern auch das Risiko erfolgreicher Angriffe durch Akteure mit umfangreichen Fähigkeiten und Ressourcen geringgehalten wird.

Neben der echten Zertifizierung wurde mit dem IT-Sicherheitsgesetz 2.0 das freiwillige IT-Sicherheitskennzeichen eingeführt und in § 9c BSIG die Befugnis zur Vergabe durch das BSI geregelt. Dieses ist keine echte Zertifizierung.[52] Gleichwohl müssen auch für die Erlangung des IT-Sicherheitskennzeichen bestimmte (Sicherheits-)Anforderungen durch die jeweiligen IT-Produkte erfüllt werden, vgl. § 9c Abs. 3 S. 1 BSIG. Dass dies der Fall ist, wird aber – anders als bei der Zertifizierung – nicht durch eine unabhängige Stelle geprüft, sondern durch den Hersteller in einer Konformitätserklärung bestätigt, § 9c Abs. 2 Nr. 1 BSIG. Das BSI prüft diese lediglich auf Plausibilität. Die Sicherheitsanforderungen an die Produkte ergeben sich gem. § 9c Abs. 3 S. 1 BSIG aus vom BSI als geeignet festgestellten Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben. Der Vorteil des IT-Sicherheitskennzeichen ist, dass der Aufwand zur Erlangung überschaubar ist, die Verbraucher damit aber die Möglich-

[50] *Glade* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 9 BSIG Rn. 2.
[51] *Glade* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 9 BSIG Rn. 50.
[52] *Glade* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 9c BSIG Rn. 9.

keit haben, zu erkennen, ob ein IT-Produkt bestimmte basale Sicherheitsanforderungen erfüllt.[53] Zudem wird neben der Konformitätserklärung mit dem IT-Sicherheitskennzeichen für ein Produkt auch eine dynamische Informationskomponente ergänzt. Denn das BSI kann auf einer Webseite zu dem jeweiligen Produkt auch Informationen über IT-Sicherheitslücken oder auch verfügbare Sicherheitsupdates für die Verbraucher veröffentlichen.[54] Dies hilft zum einen den Verbrauchern, da diese sich über Sicherheitslücken in Produkten informieren können. Es setzt aber auch einen Anreiz für Hersteller, Lücken schnell zu schließen oder sie durch bessere Produktentwicklung von vorneherein zu vermeiden.

D. Regulierungsausblick

Perspektivisch wird auch die weitere Regulierung zu Verpflichtungen führen, die mit den verschiedenen Arten der o.g. IT-Sicherheitslücken zusammenhängen und einen Beitrag zu deren Bekämpfung leisten können.

I. NIS 2-Richtlinie (EU) 2022/2555

Mit der NIS-2-RL (NIS2), (EU) 2022/2555, werden weitere IT-Sicherheitsverpflichtungen für Einrichtungen eingeführt. Ein deutlich größerer Kreis an Verpflichteten muss dann technisch-organisatorische Maßnahmen ergreifen, um IT-Sicherheitsrisiken zu beherrschen, vgl. Art. 21 Abs. 1 NIS2. Das Management und die Offenlegung von Schwachstellen – also IT-Sicherheitslücken – zählen nach Art. 21 Abs. 2 lit. e NIS2 explizit dazu. Die Verpflichteten müssen sich im Rahmen der Beschaffung entlang ihrer Lieferkette um die Sicherheit der von ihnen eingesetzten IT kümmern, Art. 21 Abs. 2 lit. d NIS2. Das gleiche gilt beim Erwerb, der Entwicklung und der Wartung von IT. Gleichwohl stellt sich die Frage, was zu tun ist, wenn man feststellt, dass es eine Lücke in einem selbst eingesetzten IT-Produkt gibt oder bei einem Cloud-Diensteanbieter. Dies insbesondere, da letzte auch durch NIS2 reguliert werden. Wie soll ein verpflichtetes Unternehmen sich ganz praktisch die Entwicklungs- oder Wartungsprozesse eines IT-Produktes anschauen, wenn es selbst kein IT-Unternehmen ist und letztlich gar nicht beurteilen kann, was da passiert? Das Unternehmen wird kaum realistisch die Chance haben, mit amerikanischen oder asiatischen Herstellern einer Software über deren sichere Entwicklungen zu reden. Selbst wenn

[53] Vgl. *Glade* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 9c BSIG Rn. 3.
[54] *Glade* in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 9c BSIG Rn. 3.

sich die Hersteller darauf einlassen, wird es den auf die IT-Sicherheit verpflichteten Kunden kaum möglich sein, die Güte der IT-Sicherheitsmaßnahmen bei der Entwicklung zu beurteilen. Denn es kann nicht jeder ein Mini-IT-Sicherheitsexperte sein. Daher sieht die NIS2 in dem Bereich auch eine Aufsicht vor. Wie das genau ausgestaltet wird, wird man sehen müssen, da die NIS2 erst noch in nationales Recht umgesetzt werden muss. Wir haben viele Aufsichtsbehörden in Deutschland. Auch nach der Umsetzung der ersten NIS-Richtlinie gab es mehrere Aufsichtsbehörden im Bereich kritischer Infrastrukturen. Teilweise ist es das BSI, teilweise ist es die Bundesnetzagentur. Wer auch immer Aufsichtsbehörde wird, darf dann auch die technische Umsetzung untersuchen und zumindest gegenüber den Betreibern der IT-Systeme Anordnungen zur Beseitigung von IT-Sicherheitslücken in einem IT-System aussprechen, vgl. Art. 32 Abs. 4 lit. b und Art. 33 Abs. 4 lit. b NIS2.

II. Cyber Resilience Act (CRA)

Mit dem Cyber Resilience Act (CRA) wird es auch neue IT-Sicherheitsverpflichtungen für Hersteller von digitalen Produkten geben. Diese sollen die IT-Sicherheit bereits bei der Entwicklung und Herstellung von Produkten berücksichtigen.[55] Zudem müssen Hersteller für einen gewissen Zeitraum sicherstellen, dass erkannte Schwachstellen geschlossen werden. Dazu gehört auch, dass die Hersteller Richtlinien für die Offenlegung von IT-Sicherheitslücken einführen und (finanzielle) Anreize für die Meldung von IT-Sicherheitslücken setzen.[56] Insofern dürfte der CRA einen wirksamen legislativen Beitrag zur Vermeidung von IT-Sicherheitslücken leisten. Auch im CRA findet sich die Erkenntnis, dass IT-Produkte heutzutage nicht mehr monolithisch von einem Hersteller entwickelt werden. Vielmehr werden viele verschiedene IT-Bestandteile, z.B. existierende Software-Bibliotheken, die von Dritten entwickelt wurden, in einem Produkt integriert. Gerade bei Open Source findet dann aber nicht unbedingt eine Pflege dieser Bestandteile statt, z.B. weil sie jemand seiner Freizeit nebenher programmiert und dann das Interesse verloren oder nicht mehr die Zeit dafür hat. Wenn dann eine IT-Sicherheitslücke in diesem Bestandteil entdeckt wird, stehen die ursprünglich Programmierenden u.U. gar nicht mehr für die Schließung der Lücke zur Verfügung. Daher verpflichtet der CRA die Hersteller von digitalen Produkten nicht nur zu einer Risikobewertung, sondern auch zur Berücksichtigung dieses Lieferkettenrisikos.[57] Diese Hersteller sollten sich also vorbereiten, damit sie selbst in der Lage sind zu agieren, wenn Sicherheitslücken in von ihnen verwendeten Bestandteilen entdeckt werden. Entweder

[55] Vgl. *Hessel/Callewaert*, K&R 2023, 789, 790.
[56] Vgl. *Hessel/Callewaert*, K&R 2023, 789, 791 f.
[57] Vgl. *Hessel/Callewaert*, K&R 2023, 789, 791.

indem sie selbst verstehen, wie diese Bestandteile ausgebaut sind, oder indem sie qualifizierte Dienstleister dafür beschäftigen, die das für sie erledigen und die Sicherheitslücken darin im Bedarfsfall schnell schließen können.

Da jede Verpflichtung nur so gut ist wie ihre Durchsetzung, sieht der CRA eine Marktüberwachung mit Untersuchungsbefugnissen vor. Die Aufsichtsbehörden dürfen sich also Produkte anschauen, z.B. wenn sie den Verdacht haben, dass sie IT-Sicherheitslücken enthalten. Sind solche Lücken enthalten, soll die Aufsicht auch die Beseitigung der Lücken anordnen können. Erfolgt diese dann nicht, kann die Aufsicht anordnen, das Produkt vom Markt zu nehmen oder zurückzurufen.[58] Hier wird sich die praktische Frage stellen, wie gut die Aufsicht angesichts der Vielzahl an digitalen Produkten skaliert. Der Erfolg wird hier im Wesentlichen von der angemessenen Ausstattung der Aufsichtsbehörden abhängen. Betrachtet man die Lage im Bereich des Datenschutzes, ist eine gewisse Skepsis angebracht, ob die Aufsicht tatsächlich immer so effektiv aufgestellt wird, dass sie mit der Vielzahl der Fälle und der Komplexität selbst großer Verfahren gegen internationale Hersteller jederzeit mithalten kann.

E. Fazit

Das BSI hat bereits eine ganze Reihe von Aufgaben und Befugnissen, um IT-Sicherheitslücken zu bekämpfen, und macht davon rege Gebrauch. Durch neue gesetzliche Regelungen auf EU-Ebene kommen neue Verpflichtungen auf Anwender, Hersteller und Importeure von IT-Produkten zu, die ebenfalls einen Beitrag zur Bekämpfung von IT-Sicherheitslücken leisten werden. Auf nationaler Ebene könnte eine Anpassung des Rechtsrahmens dafür sorgen, dass IT-Sicherheitsforschende mehr Rechtssicherheit bei ihrer Arbeit genießen und damit auch mehr zur Entdeckung und Schließung von Lücken beitragen können.

[58] Vgl. *Hessel/Callewaert*, K&R 2023, 789, 793.

Recht ohne Realisierungschance? Zur (kollektiven) Durchsetzung privater Ansprüche auf Sicherheitsupdates

Wiebke Voß

A. Einführung

Im schnelllebigen digitalen Zeitalter sind Softwareaktualisierungen aus Sicherheitsgründen omnipräsent: Das Smartphone installiert über Nacht die neueste Version des Betriebssystems zwecks „wichtige[r] Sicherheitskorrekturen“[1], der Browser spielt beim Neustart ein Auto-Update ein und Videokonferenztools wie Zoom oder Teams bestehen bisweilen im ungünstigsten Moment, just zu Beginn einer wichtigen Konferenz, auf ihrer Aktualisierung. Vielfach schon unabhängig von einer dahingehenden gesetzlichen Verpflichtung bereitgestellt, sind kostenlose Sicherheitsupdates durch die Parallelvorschriften der Art. 8 Abs. 2 Digitale Inhalte-RL und Art. 7 Abs. 3 Warenkauf-RL, umgesetzt in § 327f BGB respektive § 475b Abs. 2 BGB, nun für B2C-Verträge als Teil der geschuldeten mangelfreien Leistung verankert[2] und materiell-rechtlich durch das übliche Arsenal an Sekundärrechtsbehelfen gestützt.[3]

Die Realisierbarkeit solcher Aktualisierungsansprüche steht allerdings auf einem anderen Blatt. Die altbekannte Problematik der Durchsetzung typischerweise geringwertiger Verbraucherrechte macht vor den neuen Rechtspositionen der digitalen Welt nicht halt, im Gegenteil: Die Opazität der digitalen Technologien für den Endnutzer und Laien, im Verbund mit Konturschwächen der neuen gewährleistungsrechtlichen Vorschriften, spitzt die üblichen Hürden und Defizite individueller Rechtsdurchsetzung nur weiter zu (dazu II.). Bleiben die Ansprüche auf Sicherheitsupdates damit ein Recht ohne Realisierungschance? Wann immer die private Rechtsdurchsetzung durch den einzelnen Verbraucher derart an ihre Grenze stößt, liegt der Griff in die Kiste des kollektiven Rechtsschutzes nahe,[4] die in Umsetzung der europäischen Verbandsklagen-

[1] So etwa die Standardformulierung der iOS-Updates, bisweilen kombiniert mit „Fehlerbehebungen“ oder auch „Verbesserungen“.

[2] Im Einzelnen dazu *Riehm/Leithäuser/Brenner*, Kapitel 1, in diesem Band.

[3] Namentlich durch Nacherfüllung, Vertragsbeendigung oder Minderung sowie Schaden- und Aufwendungsersatz gem. § 327i BGB. Näher dazu *Heydn*, CR 2021, 709 (711-713); *Riehm/Abold*, CR 2021, 530; *Rieländer* GPR 2022, 28 (28-38).

[4] Vgl. die langjährige rechtspolitisch Debatte um Stärkung des kollektiven Rechtsschutzes zur wirksamen Verbraucherrechtsdurchsetzung; s. dazu *Meller-Hannich*, Gutachten A zum 72. DJT, 2018; *Basedow*, EuZW 2018, 609; *Stadler*, JZ 2018, 793.

Richtlinie unlängst um das neue Instrument der Abhilfeklage bereichert wurde. Die Möglichkeiten kollektiver Rechtsschutzinstrumente für die Realisierung von Aktualisierungsansprüchen gilt es aber kritisch auszuloten und speziell die Durchschlagskraft des neuen Verbraucherrechtedurchsetzungsgesetzes (VDuG) auf den Prüfstand zu stellen, das – so viel sei vorweggenommen – weniger als Wunderheilmittel denn als Placebo für die Rechtsdurchsetzungsproblematik daherkommt (dazu III.). Bleibt damit am Ende nur die Option, den Trend zur regulierungsrechtlichen Aufladung des Privatrechts[5] im Bereich der Cyber Resilience zurückzuschrauben und auf behördliche Durchsetzung öffentlich-rechtlicher Aktualisierungsvorgaben statt auf *private enforcement*[6] zu setzen (dazu IV.)?

B. Defizite individueller Rechtsdurchsetzung

I. Rationales Desinteresse

Vielfach erweist sich die private Rechtsdurchsetzung im Wege der Individualklage im Bereich von Updaterechten schon wegen des oft zitierten Phänomens der rationalen Apathie als ungeeignet. Angesichts des typischerweise geringen wirtschaftlichen Werts des digitalen Produkts und damit auch des Updates stehen die finanziellen und zeitlichen Ressourcen, die für ein gerichtliches Verfahren aufzuwenden wären, außer Verhältnis zum Interesse des Nutzers an einer Aktualisierung.[7] Das gilt gleichermaßen für die Durchsetzung des primären Erfüllungsanspruchs auf Bereitstellung eines Updates wie für die einschlägigen Sekundärrechte, insbesondere den (partiellen) Rückzahlungsanspruch nach Minderung gem. § 327n Abs. 4 S. 1 BGB. Selbst die Möglichkeit der außergerichtlichen Streitbeilegung nach dem VSBG überwindet die rationale Apathie der Betroffenen nur wenig;[8] auch eine Schlichtung werden Verbraucher angesichts des mit ihr verbundenen Zeit- und Kostenaufwands kaum lancieren, wenn lediglich die Aktualisierung einer Software in Rede steht.

Wo nicht bereits der geringe Streitwert den Verbraucher von einer Inanspruchnahme gerichtlichen Rechtsschutzes absehen lässt – was eher bei Waren mit digitalen Elementen der Fall sein wird als bei digitalen Produkten –, erschwert eine augenfällige,

[5] Eingehend *Hellgardt*, Regulierung durch Privatrecht, 2016, passim; s. zur Diskussion auch *Schweitzer*, AcP 220 (2020), 544 (556 ff.).

[6] Allg. zu Begriff und Konzept des *private enforcement Reimann*, Bitburger Gespräche 2008 I, 105 ff.; *Bruns*, ZZP 125 (2012), 399, 402 (405 ff.).

[7] So auch *Janal/Jung*, VuR 2017, 332 (340); *Riehm*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 201 (215).

[8] So auch *Frank/Henke/Singbartl*, VuR 2016, 333 (336).

schon im Gesetzgebungsprozess monierte[9] normative Fehlkonstruktion die Durchsetzung des Aktualisierungsanspruchs. Im typischen multipolaren Beziehungsgeflecht von Endnutzer, Zwischenhändler(n) und Hersteller normieren Richtlinien wie nationale Umsetzungsgesetzgebung allein Ansprüche gegen den Vertragspartner und Letztunternehmer in der Vertriebskette, der technisch aber nur im Ausnahmefall imstande sein wird, ein Softwareupdate zu entwickeln und bereitzustellen – sofern ihm die dazu nötige Dekompilierung des Quellcodes urheberrechtlich überhaupt als Fehlerbehebung nach § 69d Abs. 1 UrhG gestattet sein sollte.[10] Auch unterhalb der Schwelle subjektiver Unmöglichkeit, sofern der Verkäufer Einfluss auf den Hersteller nehmen und diesen als Erfüllungsgehilfen einschalten könnte,[11] macht diese Dreieckskonstruktion die Durchsetzung des Aktualisierungsanspruches jedenfalls komplex, zeitraubend und damit unattraktiv. Direktansprüche gegen den Hersteller stehen dem Nutzer hingegen nur auf Basis eines etwaig separat geschlossenen Garantie- oder Softwarepflegevertrags zu.[12] *In praxi* könnte sich der mit Sicherheitslücken konfrontierte Endnutzer eher noch zur Geltendmachung seiner Sekundärrechte veranlasst sehen; bei Sicherheitsrelevanz des unterbliebenen Updates dürfte dabei aber nur die Rückabwicklung des Vertrages, nicht aber eine bloße Minderung bei Weiternutzung des gefährdeten digitalen Produkts im Verbraucherinteresse liegen. Schadenersatzklagen gegen den Hersteller hingegen sind auf deliktischer Grundlage zwar konzeptionell denkbar, namentlich nach Ausnutzung einer Sicherheitslücke per Cyberangriff, angesichts des zu erbringenden Kausalnachweises faktisch aber kaum je ein gangbarer Weg.[13]

[9] BT-Drs. 19/31116, 6.

[10] Ungeklärt ist insoweit, ob der Verkäufer die zur Fehlerberichtigung vorausgesetzte Verwendungsberechtigung, die er durch den Weiterverkauf der Ware bzw. des digitalen Produkts an den Verbraucher verliert, von diesem ableiten kann. Näher dazu *Hoffmann/Löffler*, ZfPW 2023, 1 (9 f.); skept. auch BT-Drs. 19/27424, 27.

[11] IdS *Riehm*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 201 (214 f.); näher BeckOGK/*Riehm*, BGB, 1.8.2023, § 275 Rn. 139 f. S. auch den RegE zum Umsetzungsgesetz der DI-RL, BT-Drs. 19/27653, 58 f.

[12] Ein Updateanspruch kann sich hingegen von vornherein nicht über die Grundsätze eines Vertrags (zwischen Hersteller und Händler) mit Schutzwirkung für Dritte ergeben und resultiert auch – selbst bei tatbestandlicher Einschlägigkeit – auf Rechtsfolgenseite nicht aus ProdHaftG oder Produzentenhaftung nach § 823 Abs. 1 BGB; dazu näher *Braun*, CR 2022, 727 (733); *Schrader/Engstler*, MMR 2018, 356 (359 f.); s. auch bereits *Spindler*, NJW 2004, 3145 mwN. Etwaige Ansprüche aus Verletzung lauterkeitsrechtlicher Verkehrspflichten (dazu *Raue*, NJW 2017, 1841 (1845)) kann hingegen der einzelne Verbraucher nicht geltend machen.

[13] So auch *Mehrbrey/Schreibauer*, MMR 2016, 75 (78); *Raue*, NJW 2017, 1841 (1845).

II. Informationshürden

Neben das im Verbraucherbereich allgegenwärtige[14] Apathieproblem treten besondere informationelle Herausforderungen der digitalen Sphäre.[15] Denn als objektive Anforderung an die Vertragsmäßigkeit (§ 327e Abs. 3 Satz 1 Nr. 5 bzw. § 475b Abs. 4 Nr. 2 BGB) besteht die Pflicht zur Bereitstellung von Aktualisierungen unabhängig davon, ob sich Sicherheitsmängel auf die grundsätzliche Funktionsfähigkeit des digitalen Produktes auswirken[16] – was vielfach nicht der Fall sein wird. Dann werden die Nutzer aber von der Sicherheitslücke keine Kenntnis haben und damit auch um ihren eigenen Updateanspruch nicht wissen.[17] Sind IT-Schwachstellen hingegen erst einmal allgemein bekannt – sei es durch Herstellermaßnahmen zu ihrer Eindämmung, Sicherheitswarnungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder aufgrund prominenter Cyberattacken unter Ausnutzung der bestehenden Sicherheitsdefizite –, ist es kaum mehr die Durchsetzung des vertraglichen Aktualisierungsanspruchs, die dem Nutzer (wieder) zu einer sicheren Software verhilft: Im ersten Szenario hat der Hersteller bereits proaktiv ein Patch oder Sicherheitsupdate zur Verfügung gestellt, den Anspruch also bereits erfüllt; im zweiten und dritten wird hingegen der Marktdruck den Hersteller regelmäßig motivieren, die kritische Sicherheitslücke zeitnah per Update zu schließen, um weitere Negativschlagzeilen zu vermeiden.[18] Relevant werden Aktualisierungsanspruch bzw. Sekundärrechte deshalb im Kern nur in Fällen, in denen der Hersteller den Updatesupport für ältere Softwareversionen aufkündigt, bevor im Einzelfall der maßgebliche Zeitraum iSv § 327f Abs. 1 S. 1, § 475b Abs. 4 Nr. 2 BGB abgelaufen ist, innerhalb derer der Unternehmer zur Bereitstellung von Updates verpflichtet ist.

III. Normative und judikative Unzulänglichkeiten

Allerdings stellt die Bestimmung eben dieser Zeitspanne vor Probleme: Mit dem Novum Aktualisierungspflicht hat eine Dauerschuldkomponente Einzug in das digitale Gewährleistungsrecht (auch) punktueller Austauschverträge erhalten, der man im Kontrast zur tradierten zeitpunktbezogenen Mängelbetrachtung bestenfalls attestieren

[14] S. nur *Fries*, Verbraucherrechtsdurchsetzung, 2016, 57 f.

[15] Neben den typischen Informationshürden in der Verbraucherrechtsdurchsetzung; dazu *Voß*, in: Adrian/Evert/Kohlhase/Zwickel (Hrsg.), Digitalisierung von Zivilprozess und Rechtsdurchsetzung, 2022, 71 (79 f.); *Fries*, Verbraucherrechtsdurchsetzung, 2016, 30 ff.; s. auch *Weber*, VuR 2013, 323 (327).

[16] So auch *Braun*, CR 2022, 727 (730).

[17] *Riehm*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 201 (215).

[18] Vgl. auch die Beurteilung des *BSI*, Die Lage der IT-Sicherheit in Deutschland 2023, 33, dass Hersteller nach Entdecken einer Schwachstelle in einem IT-Produkt „in der Regel" Sicherheitsupdates bereitstellen.

mag, eine „strukturelle Schieflage“[19] auszulösen – sofern man sie nicht gleich als „Quadratur des Kreises“[20] wertet. Wie die Aktualisierungspflicht in zeitlicher Hinsicht korrekt konturiert werden kann – innerhalb welchen Zeitraums also Aktualisierungen noch bereitgestellt werden müssen, wann der Update- oder Patch-Support hingegen auslaufen darf –, kann dabei in der Sache der materiell-rechtlichen Debatte überlassen bleiben.[21] Durch die prozessuale Brille betrachtet sind es die normative Unschärfe und die damit einhergehende Rechtsunsicherheit als solche, welche die Apathie der Verbraucher und damit das Durchsetzungsdefizit verschärfen. Dass die Aktualisierungspflicht auch ihrem sachlichen Umfang nach Raum für Diskussionen lässt, namentlich in Abgrenzung zur vertraglich nicht geschuldeten Funktionserweiterung per Upgrade iSd § 327r BGB,[22] erhöht das Prozessrisiko weiter und mindert im selben Maße die Klagebereitschaft risikoavers agierender Verbraucher. In Ermangelung einer normativen Präjudizialität zivilgerichtlicher Urteile im deutschen Recht treffen diese Unsicherheiten grundsätzlich jeden Verbraucher im Individualrechtsstreit aufs Neue – jedenfalls bis zur Herausbildung einer gefestigten (höchstrichterlichen) Rechtsprechung mit der ihr eigenen faktischen Bindungswirkung.[23]

C. Rechtsdurchsetzung auf kollektiven Wegen

Derartige Defizite der individuellen Verbraucherrechtsdurchsetzung rufen beinahe reflexartig den Wunsch nach überindividuellen Klagemöglichkeiten auf den Plan. Der kollektive Rechtsschutz, der nach langem Dornröschenschlaf auf europäischer Ebene und im deutschen Recht mit Ausruf des „New Deal for Consumers“[24] und dem VW-

[19] *Riehm/Abold*, CR 2021, 530 (538).

[20] *Schöttle*, MMR 2021, 683 (686), allerdings insbes. mit Blick auf die Abgrenzung von Aktualisierung und Änderungsverbot nach § 327r BGB. S. zu den dogmatischen Bedenken auch *Bach*, NJW 2019, 1705 (1711); *Pfeiffer*, GPR 2021, 120 (125 ff.); *Wendland*, ZVglRWiss 118 (2019), 191.

[21] S. aus dem umfangreichen Schrifttum nur exempl. *Wiesemann*, MMR 2022, 343 (345 ff.); *Rieländer*, GPR 2021, 257 (268 f.); *Sosnitza*, FS Becker-Eberhard, 2022, 535 (545 ff.); *Kumkar*, ZfPW 2020, 306 (316 f.); *Wendehorst*, in: Stabentheiner/Wendehorst/Zöchling-Jud (Hrsg.), Das neue europäische Gewährleistungsrecht, 2019, 111 (129 ff.); *Braun*, CR 2022, 727 (730 f.).

[22] Dazu insbes. *Kumkar*, ZfPW 2020, 306 (317); *Schreiber/Esser*, RDi 2022, 317 (318 ff.); *Sein/Spindler*, ERCL 2019, 365 (370).

[23] Dazu *Voß*, ZZP 134 (2021), 203 (203 f.); *Maultzsch*, Streitentscheidung und Normbildung durch den Zivilprozess, 2010, 15 f., 32 f., 305 f.

[24] Bestehend aus der Mitteilung der Kommission v. 11.4.2018, COM(2018) 183 sowie dem Vorschlag der Verbandsklagenrichtlinie (COM(2018) 184, letztlich verabschiedet als RL (EU) 2020/1828) und der sog. Omnibus-Richtlinie (COM(2018) 185, verabschiedet als RL (EU) 2019/2161). Näher zum „New Deal“ *Augenhofer*, EuZW 2019, 5.

Dieselskandal verstärkt in den Fokus gerückt ist,[25] ist auch im Angesicht gerade des digitalvertraglichen Rechtsdurchsetzungsproblems schon als Retter in der Not ins Feld geführt worden.[26] Aber zu Recht, auch mit Blick auf die hier interessierenden Updateansprüche?

I. Begrenzte Wirkmacht tradierter Kollektivklageinstrumente

Die tradierten Verbandsklagen nach UKlaG und UWG sind zur Realisierung der unternehmerischen Updatepflichten respektive der Sekundärrechte bei ihrer Verletzung lediglich sehr punktuell geeignet. Zwar werden Verbraucherverträge über digitale Produkte nunmehr als kollektiv verfolgbares Verbraucherschutzrecht in § 2 Abs. 2 Nr. 1 lit. d) UKlaG in Bezug genommen,[27] sodass Verstöße gegen die verbraucherschützenden Vorschriften der §§ 327 ff. BGB, einschließlich der Aktualisierungspflicht, abmahn- und unterlassungsklagefähig sind. Die auf Unterlassung und Folgenbeseitigung zugeschnittenen Verbandsklagen nach dem UKlaG können ihrer Natur nach aber weder zur Bereitstellung eines Updates noch zu Rückzahlungen nach Minderung aufgrund von Sicherheitsmängeln verhelfen. Relevant werden kann indes das Verbandsklagerecht des § 1 UKlaG in Reaktion auf (unwirksame) Allgemeine Geschäftsbedingungen, welche die Updateansprüche der Verbraucher inhaltlich beschneiden, zeitlich verkürzen oder gänzlich abbedingen. Daneben mögen auch Verletzungen unternehmerischer Informationspflichten zur Verbandsunterlassungsklage nach § 2 Abs. 1 UKlaG Anlass geben, insbesondere sofern nach Art. 246 Abs. 1 Nr. 1 EGBGB gebotene Informationen zu wesentlichen Eigenschaften des digitalen Produkts fehlen oder unklar wiedergegeben sind. Entgegen jüngerer Rechtsprechung[28] stellen namentlich *bekannte* Sicherheitslücken sowie eine eingestellte Versorgung mit Sicherheitsupdates solche wesentlichen Eigenschaften dar, da sie erhebliche Risiken für den Nutzer und seine digitale Umgebung begründen und zusätzliche Sicherheitsmaßnahmen (etwa einen reinen Offline-Betrieb) erforderlich machen können.[29] Angesichts der als „angespannt bis kritisch“[30] einzustufenden Bedrohung durch Cyberkriminalität, die aus Kosten-Nutzen-

[25] Erhellende Bestandsaufnahme zur Entwicklung des kollektiven Rechtsschutzes im europäischen Rechtsraum bei *Stadler*, ZHR 182 (2018), 623; s. auch *Guski*, ZZP 131 (2018), 353.

[26] S. insbes. *Janal/Jung*, VuR 2017, 332 (340); *Kramme*, RDi 2021, 20 (29).

[27] In Umsetzung von Art. 23 Abs. 2 Digitale Inhalte-RL. Für den Kauf von Waren mit digitalen Elementen erübrigt sich ein separater Verweis, da Kaufverträge gem. § 2 Abs. 2 Nr. 1 lit. e UKlaG ohnehin in den Kreis umfasster Verbraucherschutzregelungen fallen.

[28] OLG Köln MMR 2020, 248.

[29] *Riehm/Meier*, MMR 2020, 250; ebenso BeckOGK/*Busch*, EGBGB, 1.7.2023, Art. 246 Rn. 18.2.

[30] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2023, 11.

Erwägungen heraus zunehmend leicht angreifbare Opfer fokussiert,[31] muss die Cyberresilienz eines Produkts mehr denn je als bedeutsamer Faktor der Verbraucherentscheidung gelten.[32]

Mit entsprechender Argumentation sind offene Sicherheitslücken und ausgelaufener Softwaresupport auch als wesentliche Informationen iSd § 5a Abs. 1 UWG einzustufen, deren Vorenthalten bei lauterkeitsrechtlicher Relevanz nach §§ 8 Abs. 1 S. 1, Abs. 3 Nr. 3, 3 Abs. 1 UWG im Verbandsklageweg verfolgt werden kann.[33] Im Übrigen unterliegen wettbewerbsrechtliche Verbandsklagen denselben Grenzen auf Rechtsfolgenseite wie ihr Pendant nach dem UKlaG. Am primären Rechtsschutzziel vorbei geht bei Verstößen gegen die Aktualisierungspflicht auch die Gewinnabschöpfungsklage des § 10 UWG. Denn wenngleich man dem Unternehmer angesichts des ersparten Aktualisierungsaufwands[34] eine Gewinnerzielung zulasten der Abnehmer attestieren mag,[35] ist die Einziehung des Gewinns doch jedenfalls subsidiär gegenüber der Erfüllung individueller Ansprüche wie vertraglichen Gewährleistungsrechten.[36] Im Hinblick auf die Aktualisierung eines digitalen Produkts ergibt sich dabei die Besonderheit, dass bereits die Befriedigung des Anspruchs eines einzelnen Nutzers den Erfüllungsaufwand in seiner Gesamtheit – nämlich die Entwicklung eines Patches – auslöst und damit den unlauter erzielten Gewinn aufzehrt.

Der Musterfeststellungsklage,[37] die mit ihrem Bedarf nach anschließender Individualklage schon im Ansatz verfehlt daherkommt,[38] fehlt schließlich jegliche praktische Wirkmächtigkeit, soweit die Durchsetzung von Aktualisierungsansprüchen in Rede steht: Auch bei vorgelagerter Klärung gemeinsamer Rechtsfragen stehen Zeit- und Kostenaufwand einer Individualklage außer Verhältnis zum Rechtsschutzziel.

---

[31] Ebd.

[32] Vgl. auch *BSI*, Die Lage der IT-Sicherheit in Deutschland 2023, 85: „Resilienz ist das Gebot der Stunde".

[33] *Riehm/Meier*, MMR 2020, 250; näher zur lauterkeitsrechtlichen Haftung der Hersteller *Raue*, NJW 2017, 1841 (1845 f.).

[34] Der RegE zum Umsetzungsgesetz der DI-RL, BT-Drs. 19/27653, 2, 28 ff. beziffert die mit der Aktualisierungspflicht einhergehenden Erfüllungskosten mit 36 Millionen Euro.

[35] Gewinn i.S.d. § 10 Abs. 1 UWG verstanden als Differenz zwischen Umsatzerlös und den zu seiner Erzielung aufgewandten Kosten; s. im Einzelnen Ohly/Sosnitza/*Ohly*, UWG, 8. Aufl. 2023, § 10 Rn. 6; Harte-Bavendamm/Henning-Bodewig/*Goldmann*, UWG, 5. Aufl. 2021, § 10 Rn. 140.

[36] § 10 Abs. 2 UWG sowie erläuternd Harte-Bavendamm/Henning-Bodewig/*Goldmann*, UWG, 5. Aufl. 2021, § 10 Rn. 173 f.

[37] Im Zuge der Umsetzung der europäischen Verbandsklagenrichtlinie überführt von §§ 606 ff. ZPO a.F. in Abschnitt 3 (§§ 41 f.) VDuG.

[38] Fundamentale Kritik an der Musterfeststellungsklage insbes. bei *Stadler*, VuR 2018, 83; *Schneider*, BB 2018, 1986; *Waßmuth/Asmus*, ZIP 2018, 657.

II. „Abhilfe" durch das VDuG?

Mit dem Gesetz zur Umsetzung der europäischen Verbandsklagenrichtlinie[39] ist der kollektive Rechtsschutz in Deutschland neu geordnet und das Trio von Unterlassungs-, Musterfeststellungs- und Gewinnabschöpfungsklage um die Albhilfeklage als vierte Rechtsschutzvariante ergänzt worden. Im Zuge der – bekanntermaßen verspäteten – Richtlinienumsetzung hat der Gesetzgeber zwar die Chance ungenutzt verstreichen lassen, den im Bereich kollektiven Rechtsschutzes wuchernden Normenwildwuchs[40] zu einem kohärenten Gesamtbild zurückzuschneiden und stattdessen bloß die Musterfeststellungsklage – terminologisch unglücklich[41] – als Form der „Verbandsklage" in das neu geschaffene Verbraucherrechtedurchsetzungsgesetz (VDuG) überführt. Aber immerhin erhält mit der Abhilfeklage, ebenfalls Regelungsgegenstand des im Oktober 2023 in Kraft getretenen VDuG, erstmals ein kollektiver Rechtsbehelf zur unmittelbaren Geltendmachung von Leistungsbegehren Einzug in das deutsche Recht, der beteiligten Verbrauchern ohne Notwendigkeit einer nachfolgenden Individualklage Befriedigung verschaffen kann: Auf Klage eines qualifizierten Verbraucherverbandes zugunsten einer Mehrzahl von Verbrauchern mit im Wesentlichen gleichartigen Ansprüchen erlässt das zuständige Oberlandesgericht[42] bei Obsiegen des Verbandes ein Abhilfegrundurteil (§ 16 VDuG) sowie – sofern nicht ein Abwicklungsvergleich geschlossen wird – ein Abhilfeendurteil (§ 18 VDuG).[43] Im anschließenden Umsetzungsverfahren obliegt es dann einem Sachwalter, die Berechtigung der teilnehmenden Verbraucher auf Basis der im Abhilfegrundurteil festgelegten Kriterien und Nachweise zu prüfen, den Unternehmer zur Erfüllung berechtigter Ansprüche aufzufordern sowie erforderlichenfalls die Verhängung von Zwangsmitteln zu beantragen.[44]

Dies ist nicht der Ort, Voraussetzungen und Wirkweise dieses neuen kollektiven Rechtsschutzinstruments in ihrer Gesamtheit nachzuzeichnen oder die konzeptionelle

---

[39] BGBl. 2023 I Nr. 272.

[40] Namentlich die erwähnten Verbandsklagen nach UWG und UKlaG, die bis dato in §§ 606 ff. ZPO a.F. geregelte Musterfeststellungsklage, die Vorteilsabschöpfung nach § 34a GWB sowie bis zum 31.8.2024 das KapMuG (s. § 28 KapMuG).

[41] Die Richtlinie bezeichnet als Verbandsklagen auf *Unterlassung oder Abhilfe* gerichtete Kollektivklagen qualifizierter Einrichtungen (vgl. die Begriffsbestimmung des Art. 3 Nr. 5 sowie Art. 7 Abs. 4 der RL); das VDuG fasst hingegen *Abhilfe- und Musterfeststellungsklagen* unter den Begriff der Verbandsklage (§ 1 Abs. 1 VDuG), ohne die weiterhin in UKlaG und UWG verorteten Unterlassungsklagen terminologisch einzubeziehen. Der Sache nach ist das Recht qualifizierter Einrichtungen, auf (Muster-)Feststellung zu klagen, freilich nicht zu beanstanden (vgl. Art. 7 Abs. 4 der RL, nach dem "mindestens" die Berechtigung zur Klage auf Unterlassungs- und Abhilfeentscheidungen bestehen muss, sowie explizit ErwGr 11).

[42] § 3 Abs. 1 VDuG.

[43] Anderes gilt im Fall der Verbandsklage auf Leistung an namentlich benannte Verbraucher, s. § 16 Abs. 1 S. 2 VDuG.

[44] § 27 Nr. 3, Nr. 10 sowie für die Zwangsmittel (nur bei anderen Forderungen als Geldforderungen) § 29 VDuG.

Verknüpfung von Verbandsklagerecht und materiell-rechtlichem Anspruch – qua eigenem Anspruch auch des Verbandes wie bei der Verbandsunterlassungsklage[45] oder bloßer Prozessstandschaft?[46] – zu beleuchten; ein umfangreiches Schrifttum nimmt sich sowohl der europäischen Richtlinie wie auch der deutschen Umsetzungsgesetzgebung bereits an.[47] Für die hier interessierenden Möglichkeiten der neuen Abhilfeklage für die Durchsetzung von Update-Ansprüchen genügt der fokussierte Blick darauf, ob diese Form der Verbandsklage auf solche Rechtspositionen anwendbar ist (a), sich konzeptionell-normativ zu ihrer gebündelten Geltendmachung eignet (b) und auch in der Praxis genutzt zu werden verspricht (c).

1. Anwendbarkeit auf Aktualisierungsansprüche

Anders als die insoweit nur mindestharmonisierende Verbandsklagerichtlinie[48] begrenzt die deutsche Umsetzungsgesetzgebung den Anwendungsbereich der Abhilfeklage von vornherein nicht auf einen Katalog einschlägiger Rechtsakte.[49] Aktualisierungsansprüche fallen damit unabhängig von ihrer Rechtsgrundlage in den Anwendungsbereich dieser Kollektivklageform – also auch solche, die nicht auf der Digitale Inhalte- oder Warenkauf-RL fußen, sondern namentlich im B2B-Bereich aus allgemeinem Vertragsrecht resultieren, insbesondere bei der Softwaremiete.[50] Auch solche Rechtspositionen von unternehmerischen Software-Nutzern können dabei im Wege der Abhilfeklage geltend gemacht werden, obschon diese nur für „Ansprüche und Rechtsverhältnisse einer Vielzahl von *Verbrauchern*“ offen zu stehen vorgibt;[51] denn

[45] S. die Anspruchsberechtigung nach § 8 Abs. 3 Nr. 3 UWG (mit Darstellung des Diskussionsstandes, ob die Norm Klagebefugnis, Aktivlegitimation oder beides regelt, bei Ohly/Sosnitza/*Ohly*, UWG, 8. Aufl. 2023, § 8 Rn. 86) sowie § 3 Abs. 1 UKlaG (zum entsprechenden Streit Köhler/Bornkamm/Feddersen/*Köhler/Alexander*, UWG, 4. Aufl. 2024, § 3 UKlaG Rn. 4).

[46] Zur Diskussion *Bruns*, Die Umsetzung der Verbandsklage-Richtlinie in deutsches Recht, 2022, 38 ff.; *Gsell/Meller-Hannich*, JZ 2022, 421 (423); *Fries*, ZZP 134 (2021), 433 (448).

[47] S. insbes. *Augenhofer*, NJW 2021, 113; *Basedow*, EuZW 2018, 609; *Biard/Kramer*, ZEuP 2019, 249; *Domej*, ZEuP 2019, 446; *Gascón Inchausti*, GPR 2021, 61; *Gsell*, BKR 2021, 521; *Gsell/Meller-Hannich*, JZ 2022, 421; *Hornkohl*, EuCML 2021, 189; *Janal*, GRUR 2023, 985; *Kern/Uhlmann*, ZEuP 2022, 849; *Meller-Hannich*, NZM 2022, 353; *Rentsch*, EuZW 2021, 524; *Röthemeyer*, VuR 2021, 43; *ders.*, VuR 2023, 332; *Scherer*, VuR 2022, 443; *Stadler*, ZHR 182 (2018), 623 (627 ff.); *dies.*, JZ 2018, 793 (800 ff.); *dies.*, ZZP 136 (2023), 129; *Thönissen*, EuZW 2023, 637; *ders.*, r+s 2023, 749.

[48] Art. 2 Abs. 1 iVm Anh. I RL (EU) 2020/1828 nimmt insbesondere auf die Digitale Inhalte-RL (Nr. 65) und Warenkauf-RL (Nr. 66) Bezug, aber etwa auch auf die Richtlinie über unlautere Geschäftspraktiken (Nr. 14), sodass auch lauterkeitsrechtliche Schadenersatzansprüche nach § 9 Abs. 2 UWG (in Umsetzung des Art. 11a UGP-RL) schon nach den europäischen Mindestvorgabe im Wege der Verbandsabhilfeklage verfolgt werden können.

[49] Zur Zulässigkeit des erweiterten Anwendungsbereichs s. ErwGr 11 RL (EU) 2020/1828.

[50] Qua mietrechtlichem Erhaltungsanspruch nach § 535 Abs. 1 S. 2 Var. 2 BGB; dazu *Riehm*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 201 (213 f.); *Wiesner*, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 10.6 Rn. 27. Zum Update als Inhalt des kaufrechtlichen Nacherfüllungsanspruchs s. BGH NJW 2022, 463 (Dieselskandal).

[51] § 1 Abs. 1 Nr. 1 VDuG [Hervorh. d. Verf.].

der deutsche Umsetzungsgesetzgeber definiert für diese Zwecke auch kleine Unternehmen mit weniger als 10 Beschäftigten und Jahresumsatz oder Jahresbilanz von höchstens 2 Millionen Euro als Verbraucher (§ 1 Abs. 2 VDuG).

Wenngleich im Fokus der Debatte um kollektiven Rechtsschutz traditionell die Kompensation von Bagatell- und Massenschäden und damit ein auf Geldzahlung gerichtetes Leistungsbegehren steht, unterliegt die Abhilfeklage keiner entsprechenden Einschränkung: Jegliches Leistungsbegehren – sei dies auf Schadenersatz, Reparatur, Ersatzleistung, Vertragsauflösung oder Erstattung des gezahlten Preises gerichtet[52] – kann im Wege der Verbandsabhilfeklage verfolgt werden (s. §§ 16 Abs. 1 S. 1, 29 VDuG), also nicht nur Schadenersatz- oder Rückzahlungsansprüche, sondern auch der Nacherfüllungsanspruch[53] auf Bereitstellung eines Updates selbst.

2. Normative und konzeptionelle Eignung

Damit ist freilich noch nicht gesagt, dass sich die neue kollektive Leistungsklage für die Durchsetzung solcher Ansprüche auch konzeptionell eignet. Zulässigkeitsvoraussetzung einer Bündelung der Verbraucheransprüche in der Verbandsabhilfeklage ist im Interesse der Effizienz auch ein hinreichendes Maß an Homogenität der betroffenen Ansprüche, das zu determinieren die Richtlinienvorlage der Verfahrensautonomie der Mitgliedstaaten überlässt.[54] In seiner finalen Fassung verlangt die dem Ähnlichkeitserfordernis gewidmete Vorschrift des § 15 Abs. 1 VDuG nur noch das Vorliegen *im Wesentlichen* vergleichbarer Sachverhalte (S. 2 Nr. 1) sowie ein entsprechendes Maß an Gleichartigkeit der entscheidungserheblichen Tatsachen- und Rechtsfragen (S. 2 Nr. 2). Die Notwendigkeit einer gänzlichen, „schablonenhaften"[55] Gleichheit der Ansprüche, wie sie der Referentenentwurf etwa auch noch im Hinblick auf Einwendungen und Einreden wie Verjährungsfragen oder den individuellen Kenntnisstand der Verbraucher postuliert hat,[56] ist damit fallen gelassen worden.[57] Im Anspruchsgrund aber werden Aktualisierungsansprüche wie auch minderungsbedingte Rückzahlungs-

[52] S. Art. 9 Abs. 1 RL (EU) 2020/1828 sowie ErwGr 5, 14, 37, 42, 50.

[53] Es mangelt insoweit freilich an einem primären Erfüllungsanspruch, wie *Pfeiffer*, GPR 2021, 120 (126) zu Recht moniert.

[54] ErwGr 12 RL (EU) 2020/1828.

[55] Regierungsentwurf BT-Drs. 20/6520, 77 f. Krit. bereits die Stellungnahmen zum Gesetzentwurf der Bundesregierung von *Allgayer*, 2; *Meller-Hannich*, 8 f. und *Röthemeyer*, 3 f.; s. auch *Dittmann/Gollnast*, VuR 2023, 135 (137); *Janal*, GRUR 2023, 985 (991 f.); *Röthemeyer*, VuR 2023, 332 (336).

[56] So ausdrücklich BT-Drs. 20/6520, 77 f.; krit. hinsichtlich der Relevanz von Verjährungsfragen auch unter dem engen Referentenentwurf allerdings *Janal*, GRUR 2023, 985 (991); vgl. auch *Mayrhofer/Koller*, ZIP 2023, 1065 (1068 f.).

[57] Dafür bereits die Stellungnahmen von *Meller-Hannich*, 8 f. und *Röthemeyer*, 3; s. auch Dittmann/Gollnast VuR 2023, 135 (137 f.); *Janal*, GRUR 2023, 985 (991 f.); *Röthemeyer*, VuR 2023, 332 (336).

ansprüche einheitlich geklärt werden können – jedenfalls mit Ausnahme der Gruppenzugehörigkeit der Verbraucher (durch Erwerb der Software), deren Prüfung aber ohnehin dem Umsetzungsverfahren vorbehalten bleibt.[58]

Allerdings bedingt das gewählte Opt-in-Modell – das von der Richtlinie zwar nur für ausländische Verbraucher diktiert,[59] in der hiesigen prozessualen Debatte aus Gründen der Gehörsgewährung aber typischerweise bevorzugt wird[60] –, dass das im Kontext individueller Rechtsdurchsetzung ausgemachte Apathieproblem nicht vollständig überwunden wird. Um von der Verbandsabhilfeklage zu profitieren, müssen Verbraucher sich der Klage durch Anmeldung ihres Anspruchs zum Verbandsklageregister aktiv anschließen (§ 46 Abs. 1 S. 1 VDuG). Trotz des verbraucherfreundlich späten Anmeldezeitpunkts[61] und der überschaubaren inhaltlichen Anforderungen an die Anmeldung[62] steht zu befürchten, dass das opt-in-basierte Verbandsklageverfahren bei geringwertigen Ansprüchen eine faktisch zu hohe Rechtsdurchsetzungshürde etabliert.[63] Die verbleibende rationale Apathie belegen Erfahrungen mit Kollektivschadenersatzverfahren nach sec. 47B Competition Act 1998 in England und Wales anschaulich: Zu den viel zitierten *collective proceedings* gegen *JJB Sports*[64] – dem einzigen Verfahren nach der ursprünglichen Opt-in-Fassung der Vorschrift – hat schätzungsweise nur jeder tausendste Betroffene seinen Individualschaden angemeldet, der aus einem Preiskartell in Bezug auf Fußball-Fanartikel resultierte und sich auf etwa 5 bis 20 GBP pro gekauftem Hemd belief.[65] Bezeichnenderweise ist im Zuge der Novellierung der Vorschrift durch den Consumer Rights Act 2015 dann die Möglichkeit eines Kollektivverfahrens auf Opt-out-Basis geschaffen worden[66] – eine Neuerung, die als Quantensprung für die

---

[58] Zur Notwendigkeit der Unterscheidung zwischen Anspruchsgrund und Einwendungen/Einreden *Thönissen*, r+s 2023, 749 (751). Zum Begriff des Anspruchsgrundes Musielak/Voit/*Musielak*, ZPO, 20. Aufl. 2023, § 304 Rn. 16.

[59] S. Art. 9 Abs. 3, Abs. 2 sowie ErwGr 45. Im Interesse einer einheitlichen Behandlung von in- und ausländischen Verbrauchern ist der gewählte Opt-in-Mechanismus auch zweckdienlich; idS auch *Janal*, GRUR 2023, 985 (989); *Nagy*, EuZW 2022, 637 (640).

[60] Vehement gegen die Opt-out-Lösung *Deutlmoser*, EuZW 2013, 652 (654); krit. auch *Stadler*, JZ 2009, 121 (129) mwN; *des.*, in: Brönneke (Hrsg.), Kollektiver Rechtsschutz im Zivilprozess, 2001, 1 (16-18). Zum Problem des rechtlichen Gehörs s. *Schauschnigg,* EuZW 2022, 1043 (1045 f.); *Rentsch*, EuZW 2021, 524 (531); sehr ausführlich auch *Stadler*, FS Schütze, 2015, 561 (569 ff.).

[61] Gem. § 46 Abs. 1 S. 1 VDuG bis zum Ablauf von drei Wochen nach dem Schluss der mündlichen Verhandlung. Zur diesbzgl. Diskussion im Gesetzgebungsverfahren *Bruns*, Stellungnahme zum Regierungsentwurf eines Gesetzes zur Umsetzung der EU-Verbandsklagenrichtlinie, 3 ff. mN; s. auch *Synatschke/Wölber/Nicolai*, ZRP 2021, 197.

[62] S. § 46 Abs. 2 VDuG.

[63] S. auch *Augenhofer*, NJW 2021, 113 (116); *Rentsch*, EuZW 2021, 524 (530).

[64] *Consumers Association v. JJB Sports (Re: Football Replica Kit)* [2009] CAT 2.

[65] Näher *Eckel*, International Review of Intellectual Property and Competition Law 46 (2015), 920 (925); *Wisking/Dietzel/Herron,* Global Competition Litigation Review 6 (2013), 68 (72); *Leskinen*, Global Competition Litigation Review 4 (2011), 79 (80).

[66] S. nunmehr Sec. 47B(7)(c),(11) Competition Act 1998; zur Reform *Williams/Bates*, Civil Justice Quarterly 38 (2019), 327.

Rechtsdurchsetzung der Kartellgeschädigten begrüßt wurde.[67] Im Hinblick auf die Aktualisierungsansprüche, zu deren Anmeldung sich viele Verbraucher auch bei sicherheitsrelevanten Produktmängeln nicht werden durchringen können, tröstet lediglich die Besonderheit, dass es für die Durchschlagskraft der Abhilfeklage nicht entscheidend auf die Zahl der angemeldeten Verbraucher ankommt: Da der Beklagte im Falle einer erfolgreichen Abhilfeklage zur Bereitstellung eines Patches verpflichtet wird und ihm die Entwicklungskosten damit ohnehin anfallen, wird er anders als bei Geldzahlungen oder analogen Leistungen kaum ein Interesse daran haben, das Update nur den teilnehmenden Verbrauchern bereitzustellen. Es steht vielmehr zu erwarten, dass die entwickelte Aktualisierung flächendeckend verfügbar gemacht wird.[68]

3. Durchschlagskraft in praxi: Das wohlbekannte Finanzierungsproblem

Erheblich beeinträchtigt zu werden droht die Durchschlagskraft der Abhilfeklage allerdings durch die Regelungen zur nunmehr als „Klageberechtigung“[69] geführten Klagebefugnis. Dass der Umsetzungsgesetzgeber die Erhebung einer Abhilfeklage in die Hände von Verbraucherverbänden legt (s. § 2 Abs. 1 VDuG) und damit ein Modell des *private enforcement* wählt,[70] ruft einen altbekannten neuralgischen Punkt auf den Plan: die finanzielle Ausstattung der klageberechtigten privaten Stellen.

Die Richtlinie beschränkt sich insoweit auf die zaghafte Vorgabe, dass die Mitgliedstaaten eine ausreichende Finanzierung sicherstellen müssten, freilich ohne konkrete Maßnahmen oder gar eine Subventionierung aus öffentlichen Mitteln zu diktieren.[71] Das vom deutschen Gesetzgeber gewählte Modell, den klageberechtigten qualifizierten Verbraucherverbänden nahezu vollständige Unabhängigkeit von Drittfinanzierern vorzuschreiben, ohne zugleich alternative Finanzquellen zu schaffen, geht aber an praktischen Realitäten gänzlich vorbei. Die gesetzliche Deckelung der Erlösbeteiligung auf 10 %[72] – mithin weit unterhalb der marktüblichen Margen von 25 bis 35 % – dürfte

[67] *Higgins/Zuckerman*, Civil Justice Quarterly 35 (2016), 1; s. auch schon *Barling*, Competition Law Journal 10 (2011), 5. Zu verbleibenden Schwächen des Kollektivverfahrens auch nach der Reform aber *Higgins*, Modern Law Review 79 (2016), 442.

[68] Es lässt sich zwar nicht ausschließen, dass lediglich den teilnehmenden Verbrauchern das Update kostenlos zur Verfügung gestellt wird, Dritten hingegen nur gegen Entgelt. Nach einer öffentlichen Verurteilung zur Bereitstellung eines sicherheitsrelevanten Patches scheint dieser Weg mit Blick auf das unternehmerische Reputationsinteresse aber wenig wahrscheinlich.

[69] Vgl. § 2 Abs. 1 VDuG. Anders noch die Terminologie bei Einführung der Musterfeststellungsklage, s. BT-Drs. 19/2439, 16, 22.

[70] Die Verbandsklagen-RL ist grds. auch für eine behördliche Rechtsverfolgung im Wege der Verbandsklagen offen, s. ErwGr 24.

[71] ErwGr 70 sowie Art. 20 Abs. 1, Abs. 2 RL (EU) 2020/1828.

[72] Gem. § 4 Abs. 2 Nr. 3 VDuG.

privatwirtschaftliche Finanzierer in den meisten Fällen bereits zuverlässig von einem Involvement abhalten.[73] Und wo mangelnde Rentabilität noch nicht zur unüberwindbaren Hürde wird, trägt die Pflicht zur vollständigen Offenlegung des Finanzierungsvertrages[74] gegenüber Gericht *und Gegner* das Ihrige zur Abschreckung potenzieller Finanzierer bei – und schafft darüber hinaus ein nicht zu rechtfertigendes prozessstrategisches Ungleichgewicht zulasten der drittfinanzierten Klägerseite.[75] Der Sorge vor unbilliger Einflussnahme seitens der Finanzierer und Interessenkonflikten im Verhältnis zu den betroffenen Verbrauchern, die ohnehin eher diffus denn empirisch untermauert daherkommt, wäre zudem in regulatorischen Vorgaben zum Finanzierungswesen besser begegnet als in Gestalt einer Zulässigkeitsvoraussetzung der Verbandsklage.[76] Modell stehen könnten dazu etwa der für die englische Finanzierergilde geltende Code of Conduct for Litigation Funders.[77]

Soweit nicht Rückzahlungs- oder Schadenersatzansprüche wegen unterbliebener Softwareaktualisierung in Rede stehen, sondern der Updateanspruch selbst, sind es freilich nicht erst diese gesetzlichen Grenzen, die eine Drittfinanzierung ausscheiden lassen. Nicht auf Geldzahlung gerichtete Klagen sind für die klassischen Prozessfinanzierer von vornherein uninteressant, da kein Erlös winkt, von dem sie anteilig profitieren könnten.[78] Eine Erstattung von Finanzierungskosten wiederum ist im VDuG nicht vorgesehen und auch die unermüdlich geforderte Stiftungslösung,[79] die auf erfolgreiche ausländische Vorbilder verweisen kann[80] und sich aus Kollektivvergleichen oder nicht abgerufenen, nach dem *cy-près*-Gedanken umgewidmeten Entschädigungsfonds finanzieren könnte,[81] ist Desiderat geblieben. Der deutsche Umsetzungsgesetzgeber verfolgt

---

[73] Ebenso *Stadler,* VuR 2023, 321 (322); s. auch *Axtmann*, DB 2023, 2614 (2615); *Heerma*, ZZP 136 (2023), 425 (432); *Schneider/Conray/Kapoor*, BB 2023, 2179 (2183, 2188) sowie die Stellungnahme des Legal Tech Verbands zum Gesetzentwurf der Bundesregierung, 7 f. (abrufbar unter www.legaltechverband.de/wp-content/uploads/2023/03/Stellungnahme_Legal-Tech-Verband_-VRUG_FIN64.pdf).

[74] § 4 Abs. 3 VDUG, in Umsetzung von Art. 10 Abs. 3 RL (EU) 2020/1828, überdies in nicht anonymisierter Form (s. § 5 Abs. 1 Nr. 4 VDuG).

[75] Krit. auch *Domej*, ZEuP 2019, 446 (466); *Stadler*, ZHR 282 (2018), 623 (652); *dies.*, VuR 2023, 321 (322); s. auch *Röthemeyer*, VuR 2021, 43 (46); *Kern/Uhlmann*, ZEuP 2022, 849 (858). Viel überzeugender insoweit der Ansatz der ELI/UNIDROIT Model European Rules of Civil Procedure, Rule 237.

[76] So zu Recht bereits *Domej*, ZEuP 2019, 446 (465).

[77] Abrufbar unter associationoflitigationfunders.com/code-of-conduct/documents/ (alle Internetquellen zuletzt eingesehen am 18.12.2023).

[78] So auch *Janal*, GRUR 2023, 985 (990); *Stadler*, ZHR 182 (2018), 623 (651); s. auch *Scheider/Conrady/Kapoor*, BB 2023, 2179 (2182).

[79] S. nur *Meller-Hannich*, Gutachten A zum 72. DJT, 2018, 60, 80; *Wagner*, Gutachten A zum 66. DJT, 2006, 14 ff.; *Röthemeyer*, VuR 2023, 332 (337); *Stadler*, VuR 2018, 83 (85); *dies.*, ZHR 182 (2018), 623 (652).

[80] S. insbes. die "Access to Justice Funds" in Ontario (www.lawfoundation.on.ca/what-we-do/access-to-justice-fund) und Québec (Bill 29/2012, ch. 3) sowie Hongkong; dazu *Mulheron*, Costs and Funding of Collective Actions, 2011, 96 ff.

[81] Näher dazu *Rinck*, Streuschadensbekämpfung in Anwendung der Cy-Pres-Doktrin, 2023; *Mulheron*, The Modern Cy-près Doctrine, Applications & Implications, 2006, passim; *Busch*, Die Cy-près-Doktrin, 2021, passim; *Mulheron*, EBLR 2009, 307; s. auch *Stadler*, ZHR 282 (2018), 623 (652).

vielmehr den schon für die Musterfeststellungsklage beschrittenen Weg der Streitwertdeckelung,[82] der allerdings die Gewinnbarkeit sachkundigen Rechtsbeistands auf Seiten der Verbände reduziert, fehlgeleitete Anreize zum Vergleichsschluss (mit höheren Anwaltsgebühren) setzt[83] und zudem nicht darüber hinwegzutäuschen vermag, dass die Verbandsabhilfeklage für die Verbraucherverbände ein Verlustgeschäft bleibt. Dafür sorgt das nie auszuschließende Prozessrisiko, das durch normative Unschärfen, wie sie bei der Aktualisierungspflicht bestehen,[84] zusätzlich verschärft wird. Die oftmals (zu) knappe öffentliche Finanzausstattung der Verbände dürfte diese deshalb gerade von riskanten – und obendrein technisch komplexen – Klagen abhalten, sodass die Durchsetzung von Updateansprüchen allzu leicht von der Agenda zu fallen droht. Beanstanden mag man zudem, dass eine Finanzierung der Verbände – und damit der Verbandsklagen – aus öffentlichen Mitteln Abhängigkeiten und Gefahren schafft, die sonst mit dem *public law enforcement* assoziiert werden, und so die Entscheidung zugunsten privater Rechtsdurchsetzung zu konterkarieren droht.[85]

D. Öffentliches Recht als Rettung?

Wenn damit auch die Abhilfeklage in ihrer letzthin verabschiedeten Gestalt dem Rechtsdurchsetzungsdefizit im Bereich von Updateansprüchen – und anderer geringwertiger Verbraucherrechte – kaum wirksam zu begegnen vermag, bleibt schließlich der hoffnungsvolle Blick in die Sphären des öffentlichen Rechts. Öffentlich-rechtliche Vorgaben mögen einerseits dazu beitragen, normative Unschärfen der neuen Verbraucherschutzvorschriften abzumildern und damit Einfluss auf die privaten Kosten- und Nutzenerwägungen im Vorfeld einer (Kollektiv-)Klage zu nehmen (dazu 1.). Andererseits mag auch die Rechtsdurchsetzung selbst in öffentliche Hände gelegt werden (dazu 2.).

I. Normkonkretisierung durch regulatorische Vorgaben

Eine materielle Regulierung des betreffenden Rechtsbereichs entfaltet normkonkretisierende Wirkung auch für private Rechtspositionen und begegnet damit dem Problem der Rechtsunsicherheit, welches die rationale Apathie von Verbrauchern erhöht und auch Verbände von der Erhebung einer Abhilfeklage abschrecken mag. Im Kontext der

[82] Gem. § 48 Abs. 1 S. 3 GKG auf 300.000 Euro für Abhilfeklagen.

[83] *Stadler*, VuR 2020, 163; im Kontext der Musterfeststellungsklage auch *Halfmeier*, ZPR 2017, 201 (204)

[84] Dazu supra II.3.

[85] *Kern/Uhlmann*, ZEuP 2022, 849 (864), unter Verweis auf das Problem des *regulatory capture*; dazu näher *Posner*, in: Carpenter/Moss (Hrsg.), Preventing regulatory capture, 2014, 49 ff.; *ders.*, Bell Journal of Economics and Management Science 5 (1974), 335.

Aktualisierungspflicht drängt sich insoweit zuvorderst der Kommissionsvorschlag für einen Cyber Resilience Act (CRA-E)[86] auf, der allgemeine Marktzugangsregeln für Produkte mit digitalen Elementen statuiert und den Hersteller *inter alia* zur kostenfreien Behebung von Sicherheitslücken während der gesamten Lebensdauer des Produkts oder – sofern kürzer – für einen 5-Jahres-Zeitraum verpflichtet.[87] Die Konformität des Produkts mit diesen Anforderungen zur Behebung von Sicherheitslücken ist nicht nur durch eine CE-Kennzeichnung des Produkts nachzuweisen;[88] diese strahlen vielmehr auch auf Vertragsbeziehungen aus, indem sie Orientierung für die berechtigten Verbrauchererwartungen an die zeitliche Bereitstellung von Aktualisierungen bieten.[89]

In dieselbe Richtung wirken die Ökodesign-Richtlinie[90] und auf ihrer Grundlage erlassene produktspezifische Durchführungsverordnungen, die zwecks Ressourcenschonung einen Mindestzeitraum festlegen, in dem Verbraucher Reparaturen erwarten dürfen.[91] Unter das von der Richtlinie verordnete „Recht auf Reparatur" fällt auch die regelmäßige Aktualisierung technischer Produkte.[92] Eine delegierte, im Juni 2023 erlassene Verordnung legt in Ausfüllung dieser Richtlinie für Mobiltelefone, Smartphones und Tablets[93] fest, dass Sicherheitsupdates mindestens noch fünf Jahre nach Beendigung des Inverkehrbringens eines Produkts (kostenlos) bereitgestellt werden müssen. Über das Scharnier der berechtigten Verbrauchererwartungen strahlen auch diese Vorgaben auf die – obschon nicht unter der Flagge der Nachhaltigkeit geschaffene – Aktualisierungspflicht nach § 327f BGB respektive § 475b Abs. 2 BGB aus.[94]

II. Public enforcement

Doch selbst unter Berücksichtigung der normkonkretisierenden Wirkung dieser regulatorischen Vorgaben bleibt die private Durchsetzung von Aktualisierungsansprüchen

[86] Verordnungsvorschlag über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

[87] S. Art. 10 Abs. 6, Abs. 12 iVm Anh. I Nr. 2 Abs. 2 sowie ErwGr. 6, 12. Näher zum Verordnungsvorschlag *Rennert*, ZfDR 2023, 206 (214) mwN.

[88] Dazu *Rennert*, ZfDR 2023, 206 (212).

[89] Zur unscharfen zeitlichen Komponente supra II.3.

[90] Richtlinie 2009/125/EG des Europäischen Parlaments und des Rates vom 21. Oktober 2009 zur Schaffung eines Rahmens für die Festlegung von Anforderungen an die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte.

[91] Näher zum *right to repair* und den produktspezifischen Durchführungsverordnungen zur Ökodesign-Richtlinie *Kieninger*, ZEuP 2020, 264 (269 ff.).

[92] Vgl. ErwGr 4, 7 RL 2009/125/EG.

[93] Verordnung (EU) 2023/1670 der Kommission vom 16. Juni 2023 zur Festlegung von Ökodesign-Anforderungen an Smartphones, Mobiltelefone, die keine Smartphones sind, schnurlose Telefone und Slate-Tablets gemäß der Richtlinie 2009/125/EG und zur Änderung der Verordnung (EU) 2023/826 der Kommission.

[94] Eingehend dazu *Specht-Riemenschneider/Mehnert*, ZfDR 2022, 313 (332 ff.).

defizitär. Zu erheblich sind die Informationsdefizite der Verbraucher wie auch der qualifizierten Verbraucherverbände in Bezug auf Sicherheitslücken und Softwarefehler,[95] zu zahnlos ausgestaltet ist die Abhilfeklage europäischer Prägung, nachdem sich der Umsetzungsgesetzgeber nicht zu einer adäquaten Finanzierung der klageberechtigten Verbände durchringen konnte.[96] Infolgedessen kann die Rechtsdurchsetzung durch Private auch nicht die Steuerungswirkung entfalten, die im so kritischen Bereich der Cybersicherheit wünschenswert wäre. Nur wenn Verstöße gegen die Pflicht zur Entwicklung und Bereitstellung von Updates ohnehin zivilgerichtlich verfolgt und geahndet werden, werden Unternehmen von vornherein davon absehen, den Aktualisierungsaufwand einzusparen, und stattdessen auf Sicherheitslücken und Softwarefehler adäquat reagieren.[97] An einer ausreichenden Prävention gegen die Vernachlässigung der Update-Versorgung besteht indes ein erhebliches öffentliches Interesse, da Softwareschwachstellen verbreitet als Einfallstor zur Kompromittierung ganzer Netzwerke genutzt werden.[98]

Wenn die Rechtsdurchsetzung durch private Akteure scheitert, drängt sich deshalb die Option auf, das *public enforcement* zu forcieren und aufsichtsbehördliche Befugnisse zu stärken. Das Behördenmodell ist zur Durchsetzung des Verbraucherrechts in anderen EU-Staaten längst an der Tagesordnung – meist gerade vor dem Hintergrund nicht hinreichend effektiver zivilrechtlicher Durchsetzung[99] – und auch hierzulande speziell für Verstöße gegen Kartell- und Kapitalmarktrecht ein bewährtes Modell.[100] Das aufsichtsrechtliche Instrumentarium reicht dabei von besonderen Ermittlungsmaßnahmen[101] über die Verhängung von Bußgeldern[102] bis hin zum Auftreten als *amicus curiae* in zivilrechtlichen Rechtsstreitigkeiten[103]. Im Bereich der Cybersicherheit ist

[95] Supra II.2. Auch Verbände verfügen typischerweise nicht über die erforderliche informationstechnologische Perspektive, wie schon der Blick in die von § 2 Abs. 1 Nr. 1 lit. a VDuG in Bezug genommene Liste der nach § 4 UKlaG klageberechtigten Verbraucherverbände nahelegt. Liste abrufbar unter https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Verbraucherschutz/Liste_qualifizierter_Einrichtungen.html.

[96] Supra III.2.c.

[97] Allg. zur unzureichenden Prävention durch private Rechtsdurchsetzung *Poelzig*; BKR 2021, 589 (591).

[98] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2023, 33, 85.

[99] *Podszun/Busch/Henning-Bodewig,* Behördliche Durchsetzung des Verbraucherrechts? Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, 2018, 66; s. auch *dies.*, GRUR 2018, 1004 (1005); *Podszun*, WuW 2017, 266.

[100] Näher dazu *Poelzig*, ZVglRWiss 117 (2018), 505 (507).

[101] Etwa die Befugnis zu Sektoruntersuchungen nach § 32e Abs. 5 GWB oder zur Durchsuchung nach § 6 Abs. 12 WpHG.

[102] S. insbes. die Sanktionstatbestände nach § 81 GWB sowie § 120 WpHG.

[103] § 90 Abs. 5 S. 1 GWB.

die behördliche Rechtsdurchsetzung zwar bereits *de lege lata* angelegt, seit das IT-Sicherheitsgesetz 2.0[104] den digitalen Verbraucherschutz als Aufgabe des BSI verankert und die Einführung eines IT-Sicherheitskennzeichens lanciert hat, das nun Orientierung bei der Bewertung von Cyber-Risiken bietet.[105] Eine Ausweitung der Befugnisse des BSI könnte aber zur Schließung der Rechtsschutzlücken beitragen. Bei Verabschiedung des Cyber Resilience Act ist ohnehin mit einer verstärkten Inpflichtnahme von Aufsichtsbehörden zur Durchsetzung der neuen Sicherheitsanforderungen für digitale Produkte zu rechnen: Der Entwurf ermächtigt die nationalen Marktaufsichtsbehörden nicht nur zur Verhängung erheblicher Bußgelder,[106] sondern auch dazu, den Rückruf von Produkten anzuordnen, welche die Marktzugangsanforderungen nicht erfüllen und deswegen ein Cybersicherheits-Risiko darstellen.[107]

E. Conclusio und Ausblick

Jahrelang ruhten die Hoffnungen für eine wirksame Durchsetzung des Verbraucherrechts auf dem kollektiven Rechtsschutz. Mit der Verbandsabhilfeklage ist nun das Arsenal von Kollektivverfahren endlich um eine unmittelbar auf Leistung zielende Klageform ergänzt worden – und doch besteht unter Verbraucherschützern zur Euphorie kein Anlass. Man würde dem deutschen Gesetzgeber reine Symbolpolitik vorwerfen, wäre er mit Verabschiedung des VRUG nicht zumindest noch seiner Pflicht zur Umsetzung der Verbandsklagenrichtlinie nachgekommen. Das Rechtsdurchsetzungsdefizit wird die Abhilfeklage mit ihrem Opt-in-Ansatz und dem wieder einmal unzureichenden Finanzierungsmodell nur in den wenigsten Fällen abfedern – und gewiss nicht in Bezug auf Updateansprüche, bei denen rationales Desinteresse, normative Fehlkonstruktion und schlichte Unkenntnis um bestehende Sicherheitslücken als toxische Mischung wirken und das Tätigwerden von Verbrauchern und Verbänden gleichermaßen hemmen.

Wenn die zivilgerichtliche Ebene, auch im Kollektiv, als Garant effektiver Rechtsdurchsetzung versagt, schlägt augenscheinlich die Stunde der Aufsichtsbehörden. Hier setzt auch der Vorschlag eines Cyber Resilience Act an, der umfangreiche Befugnisse zur Durchsetzung auch der so sicherheitsrelevanten Aktualisierungspflichten vorsieht. Allerdings: Der hier formulierte Verweis auf die behördliche Rechtsdurchsetzung, ins-

[104] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021, BGBl. 2021 I Nr. 25.

[105] Gem. § 9c BSIG; näher dazu https://www.bsi.bund.de/dok/sik-verbraucher.

[106] Beim Verstoß gegen die Pflicht zur Behebung von Sicherheitsschwachstellen nach Art. 10 Abs. 6 sind Bußgelder von bis zu 15 Millionen Euro oder bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen, s. Art. 53 Abs. 3 CRA-E.

[107] Art. 43 CRA-E.

besondere durch das BSI, gründet ausschließlich auf den Defiziten des *private enforcement*. Unterschlagen werden darf aber nicht, dass auch die Behörden sich bei der Bekämpfung von Sicherheitsrisiken mit tatsächlichen und organisatorischen Herausforderungen konfrontiert sehen, welche umgekehrt eine Betonung (auch) der privaten Durchsetzung des digitalen Verbraucherrechts nahelegen mögen.[108] Wenn öffentliche und private Rechtsdurchsetzung derart an ihren jeweiligen Gegenpart verweisen und damit die Verantwortung um digitale Resilienz von sich zu weisen versuchen, kann der Weg letztlich wohl nur über eine Stärkung *beider* Ebenen führen.

[108] Vgl. dazu die Ausführungen von *Ritter,* Kapitel 2, in diesem Band.

Compliance-Anreize durch Cyberversicherungen: Obliegenheiten zur Vermeidung von Informationssicherheitsverletzungen

Christian Armbrüster

A. Einleitung und Ausgangsthese

Der vorliegende Beitrag behandelt die Frage, inwieweit die Cyberversicherung einen Beitrag dazu leisten kann, dass die gebotenen Schutzvorkehrungen erfolgen, um das Risiko von Cyberattacken und die damit verbundenen Folgen zu reduzieren. Dabei stehen versicherungsvertragliche Obliegenheiten, also auf die Gefahrvermeidung und -reduzierung abzielende Verhaltensregeln, im Vordergrund. Dazu zählt insbesondere das Gebot, regelmäßig die verfügbaren Software-Updates vorzunehmen.

Es ist vielfach dokumentiert, dass hinsichtlich Cyber-Angriffen eine zunehmende Bedrohungslage für Gesellschaft, Wirtschaft, Staat und Verwaltung besteht. Gefahrenquellen sind dabei insbesondere Schwachstellen, die das Eindringen von Ransomware ermöglichen, offene oder falsch konfigurierte Online-Server sowie Abhängigkeiten in der IT-Supply-Chain.[1] Ein Beispiel bieten Ransomware-Attacken, die häufig über Spam-Mails mit maliziösem Anhang erfolgen; der Anhang infiziert sodann ein Opfer, das Angreifern den Zugriff auf das Unternehmensnetzwerk ermöglicht.[2]

In der Praxis werden Cyberrisiken häufig unterschätzt; zugleich wird die eigene Cybersicherheit überschätzt. Insbesondere Mittelständler wiegen sich in falscher Sicherheit.[3]

Zwischen Cybercrime und Datensicherheit besteht ein direkter Zusammenhang: Erbeutete Daten (z.B. aus Kreditkartenverträgen) werden im Darknet Interessierten zum Kauf angeboten, oder sie werden als Druckmittel für Lösegeldzahlungen verwendet. Die Fälle von Daten aus Hackerangriffen, die im Darknet aufgetaucht sind, sind

[1] BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 52. www.bsi.de. Alle zitierten Internet-Quellen wurden zuletzt am 27.10.2023 aktualisiert.

[2] BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 15. www.bsi.de.

[3] Faktenblatt Cyberkriminalität GDV 2022, S. 2. www.gdv.de.

mittlerweile Legion. Genannt seien nur Daten der Üstra (Hannoversche Verkehrsbetriebe)[4], Daten des IT-Dienstleisters des Bundes Xplain[5] oder Daten des Medienunternehmens CH Media und der NZZ.[6]

An dieser Stelle soll bereits die im Folgenden näher zu begründende These aufgestellt werden, dass die Cyberversicherung unter verschiedenen Gesichtspunkten einen erheblichen Beitrag zur allgemeinen Informationssicherheit zu leisten vermag.

B. Gesamtwirtschaftliche Funktionen von Versicherung

Es erscheint angesichts der Fragestellung sinnvoll, zunächst die gesamtwirtschaftlichen Funktionen von Versicherung in den Blick zu nehmen. Nach verbreiteter Vorstellung geht es bei Versicherung in erster Linie um die Absicherung von Individualinteressen. Das ist auch vollkommen richtig. Auf eine Kurzformel gebracht, bedeutet Versicherung gleichsam den „Tausch" eines hohen Vermögensverlustes, dessen Eintritt aber ungewiss ist, gegen einen sicheren, geringen Vermögensverlust in Gestalt der vereinbarten Prämie. Der Versicherungsnehmer vermag es dadurch, etwa das existenzbedrohende Risiko, dass sein Wohnhaus abbrennt, auf den Versicherer abzuwälzen.

Ein ganz wesentlicher Aspekt ist aber, dass Versicherung auch der Gefahrvorbeugung dient. Versicherung ist nämlich – wie noch im Einzelnen zu erörtern sein wird (s. sub III) – in der Lage, verhaltenssteuernd zu wirken. Dies beruht darauf, dass der Versicherer das Risiko regelmäßig nicht ohne Weiteres in der Gestalt als Gegenstand eines Versicherungsvertrags akzeptiert, wie es ist. Vielmehr macht er bestimmte Vorgaben, an deren Einhaltung sein Leistungsversprechen vertraglich geknüpft wird.

C. Möglichkeiten zur Verhaltenssteuerung

I. Überblick

Für die Verhaltenssteuerung stehen dem Versicherer unterschiedliche Möglichkeiten zur Verfügung. In Betracht kommt neben Prämiendifferenzierungen und Selbstbehal-

[4] https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Nach-Hackerangriff-auf-Uestra-Daten-im-Darknet-aufgetaucht,aktuellhannover14008.html.

[5] https://www.computerworld.ch/security/hacking/operative-daten-bundes-hackern-im-darknet-veroeffentlicht-2866172.html.

[6] https://www.srf.ch/news/wirtschaft/anonym-publizierte-daten-darum-ist-das-darknet-bei-hackern-so-beliebt.

ten (Eigenbeteiligungen des Versicherungsnehmers am Schaden) insbesondere die Vereinbarung von Obliegenheiten. Darunter versteht man Verhaltensvorgaben für den Versicherungsnehmer, deren Erfüllung zwar nicht einklagbar ist, bei deren Missachtung der Versicherer aber zur teilweisen oder vollständigen Leistungsverweigerung berechtigt sein kann. Es handelt sich mithin um zum Vertragsinhalt erhobene Voraussetzungen für die Erhaltung des Anspruchs auf die Leistung des Versicherers.[7] Ein alltägliches Beispiel für derartige Obliegenheiten bietet die Fahrraddiebstahlversicherung, die nur dann eingreift, wenn das Fahrrad in einer bestimmten Weise gegen Diebstahl abgesichert worden ist.

Es lässt sich unterscheiden zwischen Obliegenheiten vor, bei und nach Eintritt des Versicherungsfalls. Ein Beispiel für eine vor Eintritt des Versicherungsfalls zu erfüllende Obliegenheit bietet die sog. Winterklausel in der Gebäudeversicherung (A. 20.1.3 VGB 2022). Sie lautet wie folgt: „In der kalten Jahreszeit müssen alle Gebäude und Gebäudeteile beheizt werden. Dies ist genügend häufig zu kontrollieren. Alternativ sind dort alle wasserführenden Anlagen und Einrichtungen abzusperren, zu entleeren und entleert zu halten." Als Beispiel für bei und nach Eintritt des Versicherungsfalls eingreifende Obliegenheiten lässt sich die besondere Obliegenheit beim Verlust von Wertpapieren und Urkunden in der Hausratversicherung anführen (A 22.1 VHB 2022):

„Der Versicherungsnehmer hat bei zerstörten oder abhanden gekommenen Wertpapieren und sonstigen Urkunden etwaige Rechte zu wahren. Zum Beispiel muss er für aufgebotsfähige Wertpapiere und Urkunden unverzüglich das Aufgebotsverfahren einleiten. Ebenso muss er Sparbücher sowie andere sperrfähige Urkunden unverzüglich sperren lassen."

Die Voraussetzungen des Leistungskürzungsrechts beim Verstoß gegen eine Obliegenheit richten sich nach den Vorgaben in § 28 Abs. 2-4 VVG. Dazu zählt insbesondere das Erfordernis von grober Fahrlässigkeit oder Vorsatz. Daran zeigt sich, dass das VVG in der Tendenz sehr versicherungsnehmerfreundlich ist. Wenn die Schwelle grober Fahrlässigkeit nicht erreicht ist, bleibt ein Verstoß für den Versicherungsnehmer folgenlos. Infolgedessen kann insoweit auch keine Verhaltenssteuerung erfolgen.

Zudem steht dem Versicherungsnehmer gem. § 28 Abs. 2 S. 1 VVG die Möglichkeit des Kausalitätsgegenbeweises offen. Demnach entfällt das Leistungskürzungsrecht, wenn und soweit die Verletzung einer Obliegenheit nicht ursächlich für den Eintritt des Versicherungsfalls oder die Schadenshöhe geworden ist. Diese Beschränkungen der Vertragsfreiheit gelten nicht für sog. Großrisiken. Darunter versteht man insbesondere Versicherungsverträge, bei denen der Versicherungsnehmer zwei der folgenden drei Merkmale erfüllt: eine Bilanzsumme von mindestens 6,2 Mio EUR, Nettoumsatzerlöse

[7] Näher *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 28 Rn. 68 ff.

von mindestens 12,8 Mio EUR sowie im Durchschnitt 250 Arbeitnehmer (§ 210 Abs. 2 S. 1 Nr. 3 VVG).

Die Ausnahme für Großrisiken ist für die Cyberversicherung praktisch relevant. Freilich führt der Wettbewerb dazu, dass Versicherer auch in diesem Bereich Sanktionen für die Verletzung von Obliegenheiten üblicherweise daran knüpfen, dass der Versicherungsnehmer zumindest grob fahrlässig gehandelt hat. Bisweilen wird auf dieses Erfordernis sogar – vor allem auch jenseits von Großrisikoverträgen – gänzlich verzichtet und nur bei Vorsatz Leistungsfreiheit vorgesehen.

II. Verhaltensanforderungen durch Obliegenheiten im Vergleich zu objektiv-rechtlichen Anforderungen

Obliegenheiten reichen typischerweise in mehr oder minder großem Umfang über die gesetzlich oder behördlich vorgeschriebenen Verhaltensweisen hinaus. Ein anschauliches Beispiel bietet die Industrie-Sachversicherung, bei der dies seit jeher zu beobachten ist. Vergleicht man etwa die vertraglichen Obliegenheiten zum Brandschutz in der Industrie-Feuerversicherung mit den gesetzliche Anforderungen, so ergeben sich markante Unterschiede:

Gesetzliche Anforderungen (§ 5 – Prüfungen BGV A3 / DGUV Vorschrift 3):

> „(1) Der Unternehmer hat dafür zu sorgen, dass die elektrischen Anlagen und Betriebsmittel auf ihren ordnungsgemäßen Zustand geprüft werden
>
> 1. vor der ersten Inbetriebnahme und nach einer Änderung oder Instandsetzung vor der Wiederinbetriebnahme durch eine Elektrofachkraft oder unter Leitung und Aufsicht einer Elektrofachkraft
>
> und
>
> 2. in bestimmten Zeitabständen."

Vertragliche Obliegenheiten (SK 3602 – Elektrische Anlagen):

> „Der Versicherungsnehmer hat die elektrischen Anlagen alle __ Monate auf seine Kosten durch einen von [unternehmensindividuell ist eine vom Versicherer anerkannte Zertifizierungsstelle einzusetzen] anerkannten Sachverständigen prüfen und sich ein Zeugnis darüber ausstellen zu lassen. In dem Zeugnis muss eine Frist gesetzt sein, innerhalb derer Mängel beseitigt und Abweichungen von den anerkannten Regeln der Elektrotechnik, insbesondere von den einschlägigen VDE-Bestimmungen, sowie Abweichungen von den Sicherheitsvorschriften, die dem Vertrag zu Grunde liegen, abgestellt werden müssen."

Eine synoptische Gegenüberstellung[8] ergibt folgende teils markante Unterschiede:

Prüfung nach Klausel SK 3602	Prüfung nach DGUV Vorschrift 3
Prüfung der elektrischen Anlage hinsichtlich des **Sach- und Brandschutzes**	Prüfung der elektrischen Anlage hinsichtlich des **Personenschutzes** (Schutz gegen elektrischen Schlag)
Vereinbarung im Versicherungsvertrag durch Klausel oder andere Vertragstexte	Die Prüfung nach DGUV Vorschrift 3 ist für den **Unternehmer** in jedem Fall **verbindlich** (entsprechend § 15 des Sozialgesetzbuches SGB VII)
Ergänzungsprüfung zur DGUV Vorschrift 3 Prüfung, jedoch keine Doppelprüfung	Basisprüfung
Qualifikation des Prüfers: Nur VdS-anerkannte E-Sachverständige	Qualifikation des Prüfers: Elektrofachkraft
Vereinbarung von kurzen Prüfzyklen von ca. 1–2 Jahren	Relativ lange Prüfzyklen (im Allgemeinen alle 4 Jahre)
Mit Befundschein VdS 2229 immer gleiche Dokumentation	Unterschiedliche Prüfdokumentation möglich

Das Beispiel verdeutlicht, dass vertragliche Obliegenheiten in der Industrie-Feuerversicherung über die gesetzlichen Vorschriften zum Brandschutz deutlich hinausgehen.

III. Verhaltenssteuernde Wirkung von Obliegenheiten

Für die Ausgangsfrage ist es von Bedeutung, ob Obliegenheiten tatsächlich Auswirkungen auf das Verhalten der Versicherungsnehmer haben. Diese Frage lässt sich abstrakt dahingehend beantworten, dass Obliegenheiten in zweierlei Hinsicht wirken können:

[8] *Callondann*, s+s report 2018, 66. https://vds.de/fileadmin/user_upload/PDFs/Artikel_Warum-wir-die-Pruefung-nach-Klausel-SK-3602-brauchen_200325.pdf.

Zum einen machen sie dem Versicherungsnehmer bewusst, welche möglichen Gefahren bestehen und durch welches Verhalten diese Gefahren sich reduzieren lassen. Insoweit kommt der typischerweise bestehende Wissensvorsprung des Versicherers in denjenigen Sparten, für die er Deckungsschutz anbietet, zum Tragen.

Zum anderen bietet die Abhängigkeit des Leistungsversprechens davon, dass die Obliegenheiten eingehalten werden, einen ökonomischen Anreiz zu ihrer Einhaltung. Freilich sind – soweit ersichtlich – bislang keine empirischen Studien zu der Frage erstellt worden, in welchem Umfang diese Anreizwirkung in der Praxis tatsächlich besteht und den Versicherungsnehmer zu den nach dem Versicherungsvertrag gebotenen Verhaltensweisen motiviert. Ein empirischer Beweis für die verhaltenssteuernde Funktion von versicherungsvertraglichen Obliegenheiten und der Präventionswirkung von Normen wird im Allgemeinen grundsätzlich als schwierig erachtet.[9]

Immerhin gibt es zumindest vereinzelte Studien in ähnlichem Zusammenhang. So haben *Kötz/Schäfer* aufgezeigt, dass zwischen der Einführung des Beitragsausgleichsverfahrens und dem Rückgang der Häufigkeit der Arbeitsunfälle ein statistisch hochsignifikanter Zusammenhang besteht. Sie meinen, dass damit die Skepsis unbegründet sei, mit der in der rechtswissenschaftlichen Diskussion die verhaltenssteuernde Wirkung ökonomischer Anreize gelegentlich in Zweifel gezogen wird.[10]

Sehr eingehend hat sich jüngst *Latzel* mit der Verhaltenssteuerung im Privatrecht befasst. Er beschreibt die grundlegenden psychologischen Mechanismen der Anreizsteuerung und legt anhand von Beispielen dar, dass Anreizsteuerung gegenüber bloßer Überzeugung deutlich wirksamer ist.[11] Er untersucht auch den Einfluss der Rechtsbekanntheit auf die Rechtswirksamkeit. Dabei nimmt er an, dass es für Rechtswirksamkeit nicht der Kenntnis aller maßgeblichen Gesetze bedarf. Vielmehr genüge auch ein Rechtsempfinden und der Rückschluss von Rechtsfolgen auf die Rechtslage.[12] Diese Einschätzung lässt sich auf versicherungsvertragliche Obliegenheiten übertragen. Der Versicherungsnehmer wird diese Verhaltensanforderungen nicht immer im Detail kennen. Er wird sich aber generell dessen bewusst sein, dass er bestimmte Sicherheitsmaßnahmen ergreifen muss, um seinen Versicherungsschutz nicht zu gefährden.

Je professioneller der Versicherungsnehmer ist, umso eher wird er dabei außer den allgemein bekannten Vorkehrungen auch diejenigen Sorgfaltsanforderungen im Blick haben, die sich erst aus den Versicherungsbedingungen ergeben. Insofern dürfte in der Gewerbe- und Industrieversicherung die verhaltenssteuernde Wirkung vertraglicher Obliegenheiten bei typisierender Betrachtung stärker sein als im Verbraucherbereich.

---

[9] *Schlobach*, Das Präventionsprinzip im Recht des Schadensersatzes, 2003, S. 315. Vgl. auch *Hähnchen*, Obliegenheiten und Nebenpflichten, 2010, S. 15 ff.

[10] *Kötz/Schäfer*, Schadensverhütung durch ökonomische Anreize, AcP 189 (1989), 501, 525.

[11] *Latzel*, Verhaltenssteuerung, Recht und Privatautonomie, 2020, S. 6 f.

[12] *Latzel*, Verhaltenssteuerung, Recht und Privatautonomie, 2020, S. 478 f.

Interessant sind in diesem Kontext auch die Stellungnahmen zur verhaltenssteuernden Wirkung der Organhaftung nach §§ 93, 116 AktG, welche wiederum für die Frage der Versicherbarkeit dieser Haftung einschließlich des Selbstbehalts nach § 93 Abs. 2 S. 3 AktG bedeutsam ist. *Wagner* begreift die Vorstandshaftung ausschließlich als Instrument der Verhaltenssteuerung (und nicht der Kompensation). Aus theoretischer Sicht bestünden keine Zweifel daran, dass diese Haftung Anreize zu ökonomisch erwünschtem und sorgfältigem Verhalten setzt.[13] *Mesch* beruft sich in diesem Kontext auf das sog. Bernoulli-Prinzip.[14] Nach diesem Prinzip werden in einer Entscheidungssituation bei Risiko die zur Debatte stehenden Alternativen von einem Individuum nach ihrem Nutzenerwartungswert beurteilt. Im Ergebnis werde die nutzenmaximierende Alternative bevorzugt.

D. Marktlage zur Cyberversicherung in Deutschland

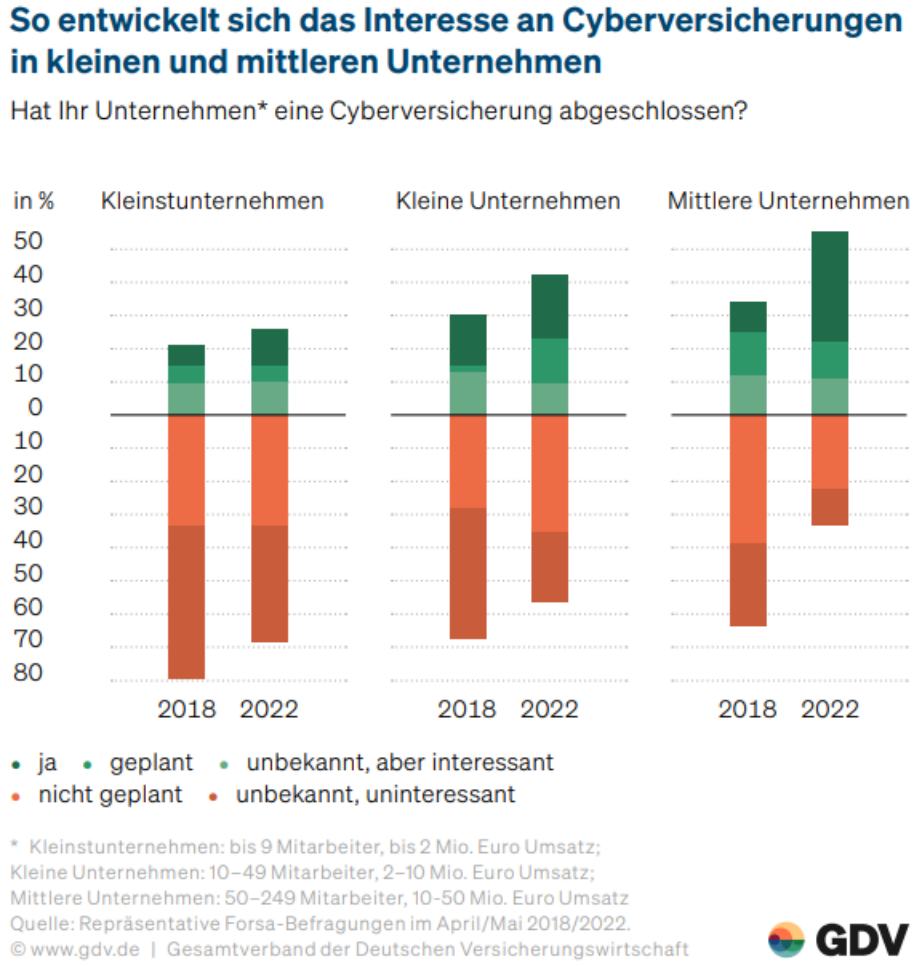
Bei größeren deutschen Unternehmen hat sich inzwischen die Erkenntnis durchgesetzt, dass eine große Bedrohungslage besteht und dass daher die Cyberversicherung eine wichtige Absicherung bietet. Bei den KMUs herrschte lange Zeit Zurückhaltung; inzwischen ist dort aber – wie auch die nachfolgende Grafik des GDV[15] zeigt – ein rasantes Wachstum zu verzeichnen. Das Prämienvolumen steigt erheblich; dies ist nicht in erster Linie auf Prämienerhöhungen zurückzuführen, sondern auf eine Steigerung der Versicherungssummen sowie der Versicherungsdichte. Ein ähnliches Bild zeichnet sich

[13] *Wagner*, ZHR 178 (2014), 227, 255 f.; dem folgend *Splinter*, Aktienrechtliche Organhaftung und D&O-Versicherung, 2021, S. 17. S. auch *Korch*, Haftung und Verhalten, 2014, S. 85 ff.

[14] *Mesch*, VersR 2015, 1337 ff.

[15] www.gdv.de.

tendenziell bei Freiberuflern ab, etwa in den rechts- und steuerberatenden Berufen oder der niedergelassenen Ärzteschaft.



E. Konzeption der Cyberversicherung

Was die Konzeption der Cyberversicherung (auch Cyberrisikoversicherung genannt) angeht, so hat der Gesamtverband der deutschen Versicherungswirtschaft (GDV) in Gestalt der Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung

(AVB Cyber) mit Stand vom April 2017 Musterbedingungen veröffentlicht.[16] Dabei handelt es sich um unverbindliche Verbandsempfehlungen. Die Allgemeinen AVB Cyber sind gerade überarbeitet worden; die Neufassung soll im Anschluss an die Gremienabstimmung im GDV bis Ende 2023 veröffentlicht werden. In der Praxis orientieren sich einige Anbieter im Grundsatz an den Musterbedingungen; es gibt aber auch zahlreiche abweichende Modelle. Im Wesentlichen sehen die Bedingungswerke üblicherweise vor, dass Eigenschäden des Versicherungsnehmers ersetzt werden. Dies betrifft etwa die Zahlung eines Tagessatzes für Betriebsunterbrechungsschäden, wenn eine laufende Produktion infolge einer Cyberattacke zum Stillstand kommt.

Ein weiterer Baustein betrifft Drittschäden, die etwa von Betroffenen eines Datenmissbrauchs oder von Abnehmern in der Lieferkette wegen Lieferverzugs gegen den Versicherungsnehmer geltend gemacht werden.

Sehr bedeutsam und im Vergleich zu anderen Versicherungssparten stark ausgeprägt ist zudem der Kostenersatz für Serviceleistungen (sog. Assistance-Leistungen). Dabei geht es etwa um den Aufwand für die Wiederherstellung der unternehmensinternen IT (Datenwiederstellung/Systemrekonstruktion) und für sonstige durch den Eintritt des Versicherungsfalls ausgelöste Maßnahmen, etwa zur Bekämpfung von Reputationsschäden. Im Bereich der Assistance kann der Versicherer etwa den Ersatz der Kosten einer IT-Forensik für Analyse, Beweissicherung und Schadensbegrenzung, der Rechtsberatung hinsichtlich IT- und datenschutzrechtlicher Informationspflichten oder des Einsatzes von PR-Spezialisten für die Krisenkommunikation[17] sowie IT-Sicherheitsschulungen versprechen.

F. Obliegenheiten in der Cyberversicherung

Vor Eintritt des Versicherungsfalls gelten nach den Musterbedingungen (A1-16 AVB Cyber) folgende Obliegenheiten: Es müssen individuelle passwortgeschützte Zugänge mit Unterscheidung von Nutzer und Befugnisebenen (Administratoren) bestehen. In der Praxis ist nach wie vor eine große Nachlässigkeit im Umgang mit Passwortänderungen zu beobachten. Dasselbe gilt für die Verwahrung der Passwörter, etwa wenn diese auf demselben Rechner abgespeichert werden, womöglich noch in einer Liste, um anderen Nutzern des Arbeitsplatzes den Zugang zu erleichtern. Dies ist hoch riskant und soll durch die Obliegenheit sanktioniert werden.

Darüber hinaus hat der Versicherungsnehmer bei Internetzugang oder mobiler Nutzung – die seit der COVID-19-Pandemie für das seitdem stark verbreitete Home-

[16] Abrufbar unter www.gdv.de. S. dazu etwa *Schilbach*, SpV 2018, 2 ff.
[17] S. dazu etwa *Dreher,* VersR 2020, 129 f.

office bedeutsam ist – zusätzliche Schutzmaßnahmen (Firewall, 2 Faktor-Authentifizierung etc.) vorzusehen. Hinzu kommt die praktisch besonders bedeutsame Obliegenheit zur automatischen Aktualisierung von Schutzmaßnahmen gegen Schadsoftware.

Des Weiteren wird ein Patch-Management-Verfahren (unverzügliche Installation von relevanten Sicherheitspatches) verlangt. Auch ein mindestens wöchentlicher Sicherungsprozess (physische Aufbewahrung) ist vorgesehen. Freilich erweisen Praxisfälle, dass der durch eine physische Aufbewahrung erzielbare Schutz begrenzt ist. Dies erweist sich insbesondere dann, wenn die Angreifer bereits die zu sichernden Dateien entsprechend manipuliert haben.

Hinzu kommen die allgemeinen Obliegenheiten, wie sie in der Sachversicherung üblich sind. Dazu zählt insbesondere die Einhaltung aller gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften (sog. Generalklausel).[18] Nicht durch diese Klausel erfasst werden privatrechtliche Regelwerke oder unverbindliche behördliche Sicherheitsvorschriften (z.B. BSI-Standards).[19] Hingegen erfasst sie die DSGVO, das BDSG und weitere datenschutzrechtliche Gesetze, die dem Schutz von (persönlichen) Daten dienen.[20]

Die nach den AVB Cyber bestehenden Obliegenheiten ergänzen und erhöhen dieses Schutzniveau deutlich (s. zu diesem Phänomen allgemein bereits oben sub III 2). Dies sei im Folgenden an einem Beispiel illustriert. Art. 32 DSGVO Abs. 1 lit. d) sieht ein „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ vor. Demgegenüber verlangt die Klausel A1-16.1 lit. d) und e) AVB Cyber „die automatische Aktualisierung von Schutzmaßnahmen gegen Schadsoftware und Patch-Management-Verfahren (unverzügliche Installation von relevanten Sicherheitspatches)“.

G. Bedeutung von Risikofragebögen

An dieser Stelle soll ein Blick auf die Bedeutung von Risikofragebögen geworfen werden. Vor dem Abschluss eines Versicherungsvertrags hat der Versicherungsnehmer häufig bestimmte risikorelevante Fragen zu beantworten. Die Antworten ermöglichen

[18] Zur Diskussion um die Transparenz dieser Klausel s. *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, AVB Cyber A1-A16 Rn. 18; *Koch*, in: Bruck/Möller, VVG, 10. Aufl. 2023, A1-16 AVB Cyber Rn. 10.

[19] *Fortmann*, r+s 2019, 429, 437.

[20] *Fortmann*, r+s 2019, 429, 437.

es dem Versicherer, das Risiko genauer einzuschätzen und über zusätzliche Obliegenheiten (teils auch als „Auflagen" bezeichnet), Risikoausschlüsse oder Prämienzuschläge zu befinden.

In vielen Versicherungssparten ist in jüngerer Zeit eine Tendenz zu beobachten, die Risikofragebögen möglichst kurz zu fassen oder sogar gänzlich darauf zu verzichten. Die Gründe dafür sind vielschichtig. Generell besteht ein Spannungsverhältnis zwischen dem Interesse des Versicherers, möglichst detailliert zu wissen, wie das von ihm zu versichernde Risiko beschaffen ist, und dem Interesse des Versicherungsnehmers an einem einfachen Vertragsschlussprozess. Knappe oder gänzlich entfallende Risikofragebögen liegen mithin im Kundeninteresse. Dies gilt keineswegs allein im Geschäft mit Verbrauchern.

Hinzu kommt, dass die dem Versicherer unabhängig von den Angaben des Versicherungsnehmers zu Gebote stehenden Instrumente zur Risikoeinschätzung immer aussagekräftiger werden. Zudem besteht ein Interesse daran, die oft für die Vertrauensbeziehung zum Kunden nachteiligen Diskussionen zu vermeiden, die entstehen können, wenn eine Falschbeantwortung von Risikofragen im Raum steht und es um die Rechtsfolgen nach §§ 19, 21 VVG geht. In Fällen, in denen sich das versicherte Risiko erst nach Vertragsschluss vergrößert, stehen dem Versicherer als Reaktionsmöglichkeit ohnehin die Regelungen zur Gefahrerhöhung nach §§ 23 ff. VVG zur Verfügung.

In der Cyberversicherung ist die Lage insofern anders, als der Versicherer hier zur Einschätzung des Risikos auf eine Vielzahl von Angaben des Versicherungsnehmers zu dessen IT-Sicherheitsstruktur angewiesen ist. Insbesondere in der Industrieversicherung können die vom Versicherungsnehmer gegebenen Antworten dem Versicherer auch Anlass bieten, Nachfragen zu stellen und ggf. zusätzliche vertragliche Obliegenheiten vorzusehen.

Der GDV hat einen unverbindlichen Muster-Fragebogen zur Risikoerfassung im Rahmen der Cyberversicherung für kleine und mittelständische Unternehmen entwickelt und veröffentlicht.[21] Im Folgenden seien hierzu zwei Beispiele genannt.

E3. Datenverarbeitung durch Dienstleister

Diese Frage dient der allgemeinen Erfassung des Geschäfts- und Risikofeldes. Vereinfachte Formulierung: „*Nutzen Sie einen Dienstleister zur Datenverarbeitung (Auftragsdatenverarbeitung nach Art. 28 DSGVO)?*"

A4. Schutz von Servern und mobilen Geräten

Diese Frage wird in Anlehnung an die Basis-Obliegenheiten gestellt. Vereinfachte Formulierung: „*Haben Sie Ihre Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen?*"

[21] www.gdv.de.

Die Konsequenzen einer Falschbeantwortung von Risikofragen sind weit reichend. Ebenso wie bei vertraglichen Obliegenheiten kann die Verletzung einer vorvertraglichen Anzeigeobliegenheit gem. §§ 19, 21 VVG bei grober Fahrlässigkeit oder Vorsatz vorbehaltlich des Kausalitätsgegenbeweises zur teilweisen oder völligen Leistungsfreiheit des Versicherers führen. Dies gilt beispielsweise dann, wenn die Frage, ob in bestimmten Abständen Sicherheitsupdates vorgenommen werden, wahrheitswidrig bejaht wird.

Rechtlich bedeutsam ist über den bei Vertragsschluss zu beantwortenden Risikofragebogen hinaus auch die umstrittene Frage, ob bei jährlichen Fragebögen während der Vertragslaufzeit gleichfalls Anzeigeobliegenheiten bestehen, für welche die §§ 19, 21 VVG gelten. Darauf soll hier nur hingewiesen werden.[22]

H. Aktuelle Judikatur

Vor kurzem hat eine Entscheidung des Landgerichts Tübingen zur Leistungspflicht des Versicherers trotz unterbliebener Software-Updates für einiges Aufsehen gesorgt. Der erste Leitsatz dieses Urteils lautet wie folgt:

> „Gelingt es, dass bei einem sogenannten ‚Pass-the-Hash'-Cyber-Angriff unter Ausnutzung einer bekannten Schwachstelle des Betriebssystems von Microsoft Administratorenrechte für alle Server des geschädigten Unternehmens erbeutet werden, lässt der Umstand, dass nicht alle Server mit den aktuellen Sicherheits-Updates ausgestattet waren, einen Leistungsanspruch gegen den Versicherer unberührt, weil eine mögliche Verletzung einer diesbezüglichen Anzeigeobliegenheit weder für den Eintritt oder die Feststellung des Versicherungsfalls noch für Feststellung oder den Umfang der Leistungspflicht ursächlich ist, es sei denn, der Versicherungsnehmer hat arglistig gehandelt."[23]

In dem zugrunde liegenden Sachverhalt ging es um Phishing. Mittels einer Phishing-Mail wurde ein Verschlüsselungstrojaner („Ransomware") eingeschleust und die gesamte IT-Infrastruktur der Versicherungsnehmerin lahmgelegt. Die Angreifer kündigten an, sensible Daten zu veröffentlichen, wenn nicht ein Lösegeld in Bitcoins gezahlt werde. Das betroffene Unternehmen hat die Lösegeldforderung zurückgewiesen und daraufhin für die Wiederherstellung der Infrastruktur – die verschlüsselt blieb und neu

[22] Ablehnend *Ulrich*, VersR 2023, 1012 ff.; differenzierend und für Schadensersatzanspruch des Versicherers *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 19 Rn. 108.

[23] LG Tübingen NJW-RR 2023, 1194. Berufung anhängig beim OLG Stuttgart (Az. 7 U 262/23).

aufgebaut werden musste – 3,8 Mio. Euro investiert. Diesen Betrag wollte es vom Versicherer ersetzt haben. Der Versicherer wandte unter anderem ein, dass der Risikofragebogen nicht zutreffend beantwortet worden sei. Das Landgericht hat sich dem im Ergebnis nicht angeschlossen. Es könne offen bleiben, ob die Versicherungsnehmerin eine grob fahrlässige oder vorsätzliche Anzeigepflichtverletzung begangen habe. Jedenfalls sei die von der Versicherungsnehmerin eingesetzte Software bereits bei Vertragsschluss veraltet gewesen und die von den Angreifern erbeuteten Administratorenrechte hätten auch bei neuerer Software einen Zugriff erlaubt. Mithin habe es für die Informationssicherheitsverletzung keine Rolle gespielt, dass die Server völlig veraltet waren und keine Sicherheitsupdates hatten. Aus Sicht des Gerichts fehlte schlicht die erforderliche Kausalität gem. § 21 Abs. 2 S. 1 VVG. Nach dieser Vorschrift steht dem Versicherungsnehmer bei einer Verletzung der Anzeigeobliegenheit der Kausalitätsgegenbeweis offen, den das Gericht hier aufgrund eines Sachverständigengutachtens für erbracht ansah.

Das LG Tübingen nahm in dem Urteil darüber hinaus auch zu der Frage Stellung, ob der Versicherungsfall grob fahrlässig herbeigeführt worden war. Das könnte nach § 81 Abs. 2 VVG zu einer Kürzung des Leistungsanspruchs führen. Das Gericht lehnte dies hier mit der Begründung ab, dass die Gefahrenlage schon bei Vertragsschluss bestanden habe, da die Server bereits damals veraltet gewesen seien. Allein darin, dass später keine Sicherheitsupdates vorgenommen wurden, liege mithin keine Herbeiführung des Versicherungsfalls. Dementsprechend heißt es im zweiten Leitsatz des Urteils:

> „Der Anwendungsbereich von § 81 Abs. 2 VVG ist dann nicht eröffnet, wenn die betreffende Gefahrenlage – hier: fehlende Sicherheitsmaßnahmen zur Vermeidung eines Cyber-Angriffs, die über den Einsatz einer Firewall und eines Anti-Viren-Scanners hinausgehen – bereits bei Vertragsschluss bestand und Grundlage der Risikoprüfung des Versicherers war bzw. hätte sein können."

Diese Ausführungen verdienen Zustimmung.[24] Der Versicherer hatte es bei den von ihm verwendeten – offenbar veralteten und jedenfalls nicht den Musterbedingungen des GDV entsprechenden – Klauseln unterlassen, dem Versicherungsnehmer hinreichend präzise Vorgaben zu machen. Der Versicherungsnehmer musste sich daher nicht an die vertraglich vorgesehenen Anforderungen halten, um den Versicherungsanspruch nicht zu gefährden. Für die Vertragsgestaltung bedeutet dies, dass der Versicherer dem Versicherungsnehmer in den AVB deutlich vor Augen zu führen hat, welche Sicherheitsanforderungen er stellt.[25]

[24] So auch Fortmann r+s 2023, 657 f.; Schilbach, VersR 2023, 1094 ff.
[25] Schilbach, VersR 2023, 1094, 1096 f.

I. Folgerungen für die Ausgangsthese

An dieser Stelle soll auf die oben (sub A) aufgestellte These, dass die Cyberversicherung im Hinblick auf das gefahrvorbeugende Verhalten des Versicherungsnehmers eine verhaltenssteuernde Wirkung entfalten kann, zurückgekommen werden. Wie dargelegt, können Verstöße gegen die Obliegenheiten zur regelmäßigen Vornahme von Software-Updates und von anderen Sicherungsvorkehrungen nur dann zu einer Leistungskürzung führen, wenn grobe Fahrlässigkeit oder Vorsatz vorliegt. In der Praxis wird aber immer wieder vor den Gerichten darüber gestritten, wann ein nachlässiges Verhalten die Schwelle zur groben Fahrlässigkeit überschritten hat.

Zudem wird der Versicherungsnehmer oft kaum im Voraus abschätzen können, ob ihm bei einem Verstoß der Kausalitätsgegenbeweis nach § 21 Abs. 2 S. 1 VVG gelingen wird. Für den Versicherungsnehmer bedeutet diese Ungewissheit, dass er eine Kürzung oder gar einen vollständigen Wegfall des Anspruchs auf die Versicherungsleistung kaum sicher wird ausschließen können, wenn er objektiv gegen die in den vereinbarten Obliegenheiten niedergelegten Sicherheitsanforderungen verstößt. Darin liegt ein Anreiz, diesen Anforderungen kontinuierlich gerecht zu werden.

Dieser Befund hat auch Folgewirkungen für die Entwickler und Hersteller von Software- und Software-Updates sowie für die sie vertreibenden IT-Dienstleister. Ein Versicherungsnehmer wird angesichts der im Cyberversicherungsvertrag vorgesehenen Obliegenheiten bei seinen für die IT-Sicherheitsstruktur verantwortlichen externen Dienstleistern darauf drängen, dass derjenige Sicherheitsstandard hergestellt und aufrechterhalten wird, der geboten ist, um den Versicherungsschutz nicht zu gefährden. Die Obliegenheiten haben damit eine Ausstrahlungswirkung auf das gesamte Umfeld, also Entwickler, Hersteller und Vertreiber der vom Versicherungsnehmer genutzten Software.

Einen zusätzlichen Beitrag zur Cybersicherheit vermag die Cyberversicherung dadurch zu leisten, dass sie ein professionelles Schadensmanagement gewährleistet. Der Cyberversicherer sorgt durch das Angebot von Assistance-Leistungen dafür, dass möglichst schnell ein wirksamer Schutz vor künftigen Cyberattacken hergestellt wird. Viele Bedingungswerke der Cyberversicherung sehen hierzu vor, dass der Versicherungsnehmer sich im Voraus mit dem Versicherer abstimmen muss, wenn er Assistance-Leistungen beauftragen möchte. Dies ist freilich angesichts des Gebots, rasch zu handeln, jedenfalls im Stadium unmittelbar nach dem Bekanntwerden einer Informationssicherheitsverletzung oftmals unpraktikabel. Dem Vernehmen nach verzichten Versicherer daher in der Praxis auch regelmäßig darauf, aus einem Verstoß gegen das vertragliche Abstimmungsgebot dem Versicherungsnehmer nachteilige Konsequenzen zu ziehen.

Nicht zuletzt ist festzuhalten, dass die Cyberversicherung die Unternehmen für die bestehenden Sicherheitsrisiken sensibilisiert. Dadurch, dass diese Risiken im Vorfeld

des Vertragsschlusses angesprochen werden, wird dem jeweiligen Unternehmen verdeutlicht, dass es eine Bestandsausnahme machen und Instrumente vorsehen muss, um den Obliegenheiten gerecht zu werden, etwa indem die nötigen Updates sichergestellt werden. In der Gewerbe- und Industrieversicherung stehen dem Versicherungsnehmer dabei in der Praxis regelmäßig Versicherungsmakler mit spezieller Expertise im Cyberversicherungsmarkt beratend zur Seite.

J. Fazit und Ausblick

Als Fazit lässt sich festhalten, dass die Existenz der Cyberversicherung und insbesondere die darin vorgesehenen Obliegenheiten Betroffene für Sicherheitsrisiken zu sensibilisieren vermögen. Zugleich setzt die Vertragsgestaltung ökonomische Anreize dafür, Sicherheitslücken zu vermeiden oder zu beheben. Auch nach Eintritt des Versicherungsfalls kann die Cyberversicherung durch professionalisierte Begleitung bei der Minimierung der Schäden helfen und künftigen Informationssicherheitsverletzungen vorbeugen. Damit leistet sie einen wesentlichen Beitrag zur allgemeinen Informationssicherheit.

Freilich besteht ein Spannungsverhältnis zwischen dem (notwendigen) Komplexitätsgrad der Produkte und den Bedürfnissen der Versicherungsnehmer nach leicht verständlichem und handhabbarem Versicherungsschutz. Dem hat die Vertragsgestaltung Rechnung zu tragen.

Künftig sind weitere Entwicklungen des dynamischen und heterogenen Marktes für Cyberversicherungen zu erwarten. Was die rechtliche Beurteilung der AVB angeht, so sind gerichtliche Klärungen zu erwarten, etwa im Hinblick auf die beim OLG Stuttgart eingelegte Berufung gegen das Urteil des LG Tübingen, das eine Pflicht des Versicherungsnehmers zu laufenden Sicherheits-Updates mangels hinreichend präziser Vorgaben in den AVB verneint hat (s. sub VIII). Das allgemeine Schutzniveau im Bereich der Cybersicherheit dürfte auch durch die Gesetzgebung weiter angehoben werden. So steht bis Oktober 2024 die Umsetzung der europäischen NIS-2-Richtlinie (2022/2555) zur Netzwerk- und Informationssicherheit[26] an, die Neuerungen zumindest für mittlere Unternehmen und kritische Infrastruktur bringen wird.

[26] https://eur-lex.europa.eu/eli/dir/2022/2555.

Autorenverzeichnis

Christian Armbrüster
Professor für Bürgerliches Recht, Handels- und Gesellschaftsrecht, Privatversicherungsrecht und Internationales Privatrecht, Freie Universität Berlin.

Christian Ernst
Professor für Öffentliches Recht und Wirtschaftsrecht einschließlich Vergaberecht, Helmut-Schmidt Universität Hamburg.

Benjamin Raue
Professor für Zivilrecht, Recht der Informationsgesellschaft und des Geistigen Eigentums, Universität Trier und Geschäftsführender Direktor des IRDT.

Thomas Riehm mit Malte Leithäuser und Raphael Brenner
Professor für Deutsches und Europäisches Privatrecht, Zivilverfahrensrecht und Rechtstheorie sowie dessen wissenschaftliche Mitarbeiter, Universität Passau.

Steve Ritter
Referatsleiter für IT-Sicherheit und Recht, Bundesamt für Sicherheit in der Informationstechnik Bonn.

Wiebke Voß, LL.M. (Cambridge)
Juniorprofessorin für Bürgerliches Recht, Universität Würzburg.

Thomas Wischmeyer
Professor für Öffentliches Recht und Recht der Digitalisierung, Universität Bielefeld.

SCHRIFTEN DES IRDT

TRIER STUDIES ON DIGITAL LAW

Benjamin Raue (Hrsg.)

Digitale Resilienz: Effektives Recht auf sichere Software

Volatilität, Unsicherheit, Komplexität und Ambiguität prägen das aktuelle Weltgeschehen. Das wirkt sich auf digitale Systeme aus, die zunehmend anfällig für Bedrohungen und Störungen sind. Mit der fast flächendeckenden Verbreitung digitaler Technologien steigen Risiken durch Fehlfunktionen und Datenmanipulationen. Die Folge sind Ransomware oder andere Cyberattacken. Ziel ist daher, die digitale Resilienz zu erhöhen. Damit gehen technische und rechtliche Herausforderungen einher, insbesondere wie Sicherheitslücken geschlossen und insgesamt die Sicherheit von Software erhöht werden kann.

Dieser Band adressiert folgende Themen:

- Sicherheit und Sicherheitslücken
- Vertragliche Ansprüche auf Sicherheitsaktualisierungen
- Staatliche Verantwortung für sichere Software
- Die Rolle des BSI in der Bekämpfung von Sicherheitslücken
- Durchsetzung privater Ansprüche auf Sicherheitsupdates
- Compliance-Anreize durch Cyberversicherungen